# INSIKA-Demonstration
# Schnellstart-Anleitung

letzte Änderung: 26.02.2010

Status: vorläufig

# Hinweis zum Dokument

Diese INSIKA-Dokumentation enthält als Ergänzung zur Spezifikation der TIM-Schnittstelle eine kurzgefasste Einführung in die Materie, Hinweise zu Bedienung der Demonstrations-Software sowie für eine praktische Implementierung.

Das Dokument wendet sich vor allem an zwei Zielgruppen: (1) an Personengruppen, die das System anhand der Demonstrations-Software besser kennen lernen und (2) an Entwickler, die ein TIM in bestehende oder neue Produkte integrieren wollen bzw. sich einen Überblick über das richtige Vorgehen und den Aufwand verschaffen möchten.

Mit der Veröffentlichung der Dokumentation können sich Interessierte über die Grundlagen der INSIKA-Technik informieren und sind damit prinzipiell in der Lage, das Konzept praktisch umzusetzen. Die dargestellten Verfahren, Modelle und Schnittstellen haben weder den Charakter von Normen oder Vorschriften noch sind sie derzeit Gegenstand gesetzlicher Regelungen.

Um schnell über Änderungen informieren zu können, wird die Dokumentation nur an registrierte Unternehmen ausgegeben. Das INSIKA-Konsortium geht allerdings davon aus, dass bereits jetzt eine stabile Version ohne wesentlichen Änderungsbedarf vorliegt.

Aus den in dieser Beschreibung dargestellten technischen Inhalten können keine Garantien oder Verpflichtungen abgeleitet werden. Die Autoren und das Konsortium übernehmen bei Übernahme oder Benutzung des Konzeptes oder von Teilen davon keine Haftung oder Verantwortung.

Eine entwicklungsbegleitende Unterstützung von Implementierungen ist momentan nicht möglich. Fragen zum Konzept werden im Rahmen der Möglichkeiten beantwortet. Das INSIKA-Konsortium wird über den weiteren Projektablauf kontinuierlich informieren.

Das INSIKA-Projekt wird vom Bundesministerium für Wirtschaft und Technologie unter der Fördernummer MNPQ 11/07 gefördert.

Projektinformationen: http://www.insika.de/

# Änderungshistorie

| Version | Datum | Änderung | Anmerkung |
|---|---|---|---|
| 1 | 12.02.2010 | | Initiale Version |
| 0.1.2 | 26.02.2010 | | Ausgabeversion |

Autoren: J. Reckendorf, N. Zisky, J. Wolff, J. Neumann

Kontakt: Physikalisch-Technische Bundesanstalt (PTB)
FB 8.5, INSIKA-Projekt
Abbestraße 2-12
10587 Berlin
insika@ptb.de

Dateiname: INSIKA_Quickstart_v_0.1.2.doc
Version: 0.1.2
Referenzierte TIM-Applikation: T.1.0.6.
Status: vorläufig
Letzte Änderung: 26.02.2010

# Inhaltsverzeichnis

# 1 Einführung

## 1.1 INSIKA - Überblick

Die Abkürzung INSIKA steht für „INtegrierte SIcherheitslösung für messwertverarbeitende KAssensysteme“. Diese Lösung wird in einem Projekt unter Leitung der PTB zur Serienreife entwickelt.

Die Anwendung des INSIKA-Konzepts stellt die lückenlose, revisionssichere Aufzeichnung von Einzelbuchungen bei Bargeschäften unter Nutzung einer elektronischen Registrierkasse sicher. Die INSIKA-Technik ist ein neuer Ansatz zum Nachweis der Ordnungsmäßigkeit der Buchführung. Anders als bei „klassischen“ Fiskalsystemen mit aufwändigen, technischen Speziallösungen, die meist Daten in mechanisch gesicherten (z.B. verplombten) Speichermodulen ablegen, resultiert die Sicherheit aus den kryptografisch gesicherten Buchungsdaten selbst.

Zur Nutzung des Konzepts ist eine Registrierkasse erforderlich, die eine spezielle Smartcard nach eindeutig festgelegten Regeln ansteuert und die alle mit Hilfe der Smartcard erzeugten Daten zusammen mit den Daten der Buchung in ein Standardformat umwandelt.

Der Schutz der so erzeugten Daten erfolgt mit hochsicheren IT-Standardverfahren. Anforderungen an die Bauart - und insbesondere die Sicherheit der Registrierkasse - gibt es nicht. Die Sicherheit des INSIKA-Systems resultiert aus evaluierten Schutzmechanismen der Smartcard und der darauf aufgebrachten Software und Schlüssel.

Ein Einstieg in die INSIKA-Technik ist einfach. Jeder, der über grundlegende PC-Kenntnisse verfügt, kann die wesentlichen Abläufe nachvollziehen. Die Nutzung/Evaluierung des Systems erfordert keine Spezialkenntnisse.

Die INSIKA-Projektgruppe stellt als Ergebnis von zwei Jahren Projektlaufzeit Interessenten ein vollständiges Demonstrationspaket vor. Im Projekt entwickelte Komponenten (Smartcard) können von Interessierten angefordert werden. Unter Nutzung der Smartcard lassen sich alle Prozessabläufe nachvollziehen. Das sind im Einzelnen:

- Bereitstellung von INSIKA-Smartcards (Personalisierung einschl. Zertifikat)
- Erzeugung von signierten Kassendaten (mit einem speziell dafür entwickelt Kassensimulator oder auch mit bestehenden, entsprechend angepassten Kassensystemen)
- Verifikation von INSIKA-Buchungsdaten

Aufwand und Kosten zur Entwicklung von Kassensystemen mit INSIKA-Funktionalität und Prüfmethoden sind damit gut abschätzbar. Im Abschnitt 1.3 („Zielgruppen“) findet sich ein Überblick zu den Zielgruppen der jeweiligen Abschnitte dieser Dokumentation.

## 1.2 Erforderliche Komponenten für INSIKA-Demonstration

Zur Demonstration von INSIKA auf einem Windows-PC sind folgende Komponenten erforderlich:

- Smartcard (mit spezieller Software, diese Einheit wird als „TIM“ = „Tax Identification Module“ bezeichnet) mit Zertifikat: Diese Karte kann auf Anforderung jedem Interessenten zu Testzwecken zur Verfügung gestellt werden.
- Kartenleser mit USB: Standardkartenleser für Smartcards ohne spezielle Sicherheitsanforderungen, Treibersoftware für Kartenleser gehört zum Lieferumfang des Kartenlesers.
- INSIKA Demonstrations Software:
  - Kassensimulator: Spezialprogramm zur Erzeugung von INSIKA-Kassendaten einschließlich Kurzanleitung zur Bedienung des Programms. Diese Software wird Interessenten zu Testzwecken kostenlos zur Verfügung gestellt. Das Programm stellt nur einfache Kassenfunktionen zur Verfügung. Die gespeicherten Daten entsprechen jedoch vollständig der INSIKA-Spezifikation.
  - Prüfsoftware von INSIKA-Buchungsdaten (IVM): Mit dieser Software können unabhängig von der Kassensoftware die INSIKA-Buchungsdaten auf ihre Unversehrtheit hin überprüft werden
  - TIM-Browser: Programm zum Auslesen von Informationen aus dem TIM

## 1.3 Zielgruppen

### 1.3.1 Kassenanwender

Kassenanwender können sich mit dem Demopaket schnell einen Überblick über das INSIKA-System verschaffen, den Aufwand einer Umstellung und die Auswirkung im täglichen Betrieb bewerten.

Es wird empfohlen, mindestens die folgenden Abschnitte dieser Dokumentation (und jeweils die dort erwähnten anderen Dokumente) zu lesen:

- 2.2.1: Wesentliche Zusammenhänge
- 2.3: Unterschiede zu klassischen Fiskalspeichern
- 3: INSIKA-Demonstrator
-

### 1.3.2 Hersteller (Kassensysteme, Hardware und Software)

Hersteller können unter Nutzung von Protokollierungsfunktionen der Kassensimulatorsoftware die in den Schnittstellenspezifikationen festgelegten Details einfach nachvollziehen. Damit ist ein schneller Einstieg in die INSIKA-Technik möglich. In Kombination mit der Prüfsoftware können Vorgehensweise und Aufwand für eine Integration der INSIKA-Smartcard in eine eigene Kassenumgebung leicht bewertet werden. Eine vollständige Einbindung in bestehende oder neue Produkte ist ebenfalls möglich.

Es wird empfohlen, mindestens die folgenden Abschnitte dieser Dokumentation (und jeweils die dort erwähnten anderen Dokumente) zu lesen:

- 2: Grundlagen
- 4: Implementierung in Kassensysteme

### 1.3.3 Betriebsprüfer, Steuerberater, Wirtschaftsprüfer

Betriebsprüfer, Steuerberater oder Wirtschaftsprüfer können sich innerhalb kurzer Zeit in die INSIKA-Technik vollständig einarbeiten, da die INSIKA-Daten beliebiger Hersteller durch das einheitliche Exportformat eindeutig festgelegt sind. Damit entfällt die sonst erforderliche Analyse der jeweils verwendeten Datenstrukturen und -formate.

Es wird empfohlen, mindestens die folgenden Abschnitte dieser Dokumentation (und jeweils die dort erwähnten anderen Dokumente) zu lesen:

- 2.2: Grundkonzept
- 3: INSIKA-Demonstrator

### 1.3.4 Entscheider in Politik, Verwaltung und Wirtschaft

Entscheidungsträger, die sich eine Meinung über das INSIKA-System bilden möchten, können sich mit dieser Dokumentation einen schnellen Überblick über Funktionsweise, Sicherheit und die wichtigsten Aspekte für eine Kostenbetrachtung verschaffen. Diese Aspekte werden im Abschnitt 2 („Grundlagen“) behandelt.

Eine etwas weitergehende Einarbeitung anhand der Demonstrations-Software (Abschnitt 3) ist empfehlenswert.

## 1.4 Aufgaben Demopaket

Das Demopaket soll allen Zielgruppen durch Ausprobieren und Nachvollziehen der einzelnen Schritte einen raschen Einstieg in die INSIKA-Technik ermöglichen. Auf dieser Grundlage sind Entscheidungen besser zu treffen als bei reiner Prüfung der Dokumentationen.

Auch Nichttechniker können sich durch den Umgang mit einem realen System sehr schnell einen guten Überblick verschaffen.

Ab Frühjahr 2010 werden Kassenprototypen einem Feldversuch unterzogen. Über die Ergebnisse dieser Feldversuche und die Reaktion auf die Arbeit mit dem INSIKA-Demopaket wird das INSIKA-Konsortium in regelmäßigen Abständen berichten.

Die Einbindung der INSIKA-Smartcard in ein bestehendes modernes Kassensystem, insbesondere in PC-basierte Systeme, ist nach bisherigen Erfahrungen relativ schnell und kostengünstig durchführbar.

# 2 Grundlagen

## 2.1 Ursprünge des INSIKA-Projektes

Im Jahresbericht 2003 des Bundesrechnungshofes wurde auf drohende Steuerausfälle durch Manipulationsmöglichkeiten in modernen Registrierkassen hingewiesen. In Registrierkassen gespeicherte Daten können in vielen Systemen beliebig, ohne die geringsten Spuren zu hinterlassen, verändert werden. Abhilfe ist demnach dringend geboten.

Deshalb erarbeitete das BMF einen Gesetzentwurf zur Verhinderung dieser Manipulationen unter Bezug auf ein von der Physikalisch-Technischen Bundesanstalt (PTB) und dem Bundesministerium für Finanzen erarbeiteten Verfahren. In einer Bund-Länder-Arbeitsgruppe „Registrierkassen“ wurde ein Fachkonzept zur Umsetzung des Gesetzes entwickelt. Unter Leitung der PTB wird eine entsprechende technische Lösung im Rahmen des INSIKA-Projektes konzipiert und umgesetzt. Der Gesetzentwurf wurde im Juli 2008 vorgelegt, dann aber wieder zurückgezogen. In mehreren europäischen Ländern gibt es grundsätzliches Interesse an der INSIKA-Lösung.

Das Gesamtkonzept und die Spezifikation aller Schnittstellen werden vollständig offen gelegt. Es besteht keinerlei Patentschutz. Für die Nutzung des Konzepts werden keine Lizenzgebühren o.ä. erhoben. Es entstehen bei einem Einsatz des Systems also keinerlei grundlegende Abhängigkeiten. Die im Rahmen des Projekts in Kassen implementierte Software unterliegt jedoch dem Urheberrecht der jeweiligen Firmen, es handelt sich nicht um Open-Source oder Freeware.

Das Projekt wird vom Bundesministerium für Wirtschaft und Technologie im Rahmen des Förderprogramms "Unterstützung kleiner und mittlerer Unternehmen bei der Umsetzung von Innovationen in den Bereichen Messen, Normen, Prüfen und Qualitätssicherung" ("MNPQ-Transfer") maßgeblich unterstützt.

## 2.2 Grundkonzept

### 2.2.1 Wesentliche Zusammenhänge

Der Manipulationsschutz basiert vor allem auf einer elektronischen Signatur, die von einer durch eine autorisierte zentrale Stelle ausgegebenen Smartcard mit spezieller Software (dem TIM) erzeugt wird. Damit geschützte Daten können nicht unerkannt verändert werden. Selbst bei einer Manipulation oder beim Verlust der Daten ist durch technische Vorkehrungen noch eine Abschätzung der Umsätze möglich.

Mit elektronischen Signaturen lässt sich sicher feststellen, dass Daten von einer bestimmten Person oder einem System (hier: einer ganz bestimmten Registrierkasse) stammen und dass die Daten seit Erstellung der Signatur nicht verändert wurden. In den meisten Anwendungsfällen – wie auch im INSIKA-System – werden Smartcards zur Erzeugung der Signaturen eingesetzt.

Für das System werden handelsübliche Smartcards verwendet, die mit einer speziellen Software ausgestattet sind und als „TIM“ bezeichnet werden. Diese sollen bei Umsetzung des Gesetzes von der Finanzverwaltung in einem offenen Ausschreibungsverfahren beschafft und an Steuerpflichtige auf Antrag ausgegeben werden.

Das TIM kann über einen externen Kartenleser angeschlossen oder in das Gerät integriert werden (wie z.B. bei Mobiltelefonen). Die Software der Registrierkasse muss das TIM entsprechend ansteuern und den Ausdruck sowie die Speicherung der Daten gewährleisten. Darüber hinaus gehende Änderungen an der Registrierkasse sind nicht erforderlich. Der größte Teil der am Markt befindlichen Registrierkassen und Kassensysteme kann ohne großen Aufwand nachgerüstet werden.

Gedruckte Kassenbelege und die zugehörigen, elektronisch gespeicherten Buchungen werden mit einer elektronischen Signatur versehen. Diese Signatur wird vom TIM erstellt. Ferner führt das TIM einen internen Zähler, der sicherstellt, dass jede Buchung und der dazugehörige gedruckte Beleg eine eindeutige und fortlaufende Nummer ("Sequenznummer") erhält.

Zusätzlich werden im TIM Summenspeicher verwaltet, welche die Gesamtumsätze so erfassen, dass im Falle des Verlustes von gespeicherten Daten wesentliche Kennzahlen (Monatsumsätze, negative Buchungen usw.) ermittelt werden können. Die Erzeugung der Signaturen und die Verwaltung von Sequenzzähler und Summenspeichern sind im TIM so miteinander verknüpft, dass bei Erzeugung einer Signatur eine neue Sequenznummer vergeben wird und die Summenspeicher aktualisiert werden.

Über einen Belegausgabezwang und die Verpflichtung, dass jeder Beleg eine gültige Signatur tragen muss, ist somit die korrekte Aufzeichnung der Daten sichergestellt, da alle weiteren Schritte über Verknüpfung der verschiedenen Funktionen innerhalb des TIM erzwungen werden.

Damit werden im Wesentlichen nur die Daten gespeichert, zu deren Aufbewahrung der Steuerpflichtige ohnehin heute bereits verpflichtet ist. Neu ist die lediglich Aufbewahrungsverpflichtung der zusätzlichen Signaturen und Sequenznummern für jede Buchung.

Jegliche Prüfung der Kassendaten nutzt die gespeicherten und signierten Buchungen. Da diese Daten nicht unerkannt veränderbar sind, bleiben alle erdenklichen Manipulationen an den sonstigen Kassenberichten oder den Stammdaten der Registrierkasse wirkungslos, da sie durch einen einfachen Vergleich mit den abgesicherten Buchungsdaten sofort auffallen. Selbst durch bewusst in eine Registrierkasse integrierte Manipulationsfunktionen kann das System nicht angegriffen werden, weshalb eine aufwändige Zertifizierung der Geräte überflüssig ist.

Die Prüfung der aufgezeichneten Daten kann in weiten Teilen automatisiert werden und ist damit wesentlich effizienter als in der Vergangenheit.

Die Prüfung gedruckter Belege erfordert lediglich Informationen, die auf dem Ausdruck vorhanden sind. Es ist kein Rückgriff auf die gespeicherten Buchungsdaten erforderlich. Somit ist bei jedem gedruckten Beleg leicht zu überprüfen, ob dieser durch eine Registrierkasse mit gültigem TIM erstellt wurde. Jede falsch erstellte Rechnung ohne oder mit ungültiger Signatur stellt einen eindeutigen Beweis für eine Manipulation dar.

Steuerpflichtige können mit dem INSIKA-System die korrekte Erfassung und die unveränderte Speicherung der mit der Registrierkasse erfassten Daten belegen.

### 2.2.2 Kryptografie

Für das INSIKA-Verfahren geeignete elektronische Signaturen werden mit so genannten asymmetrischen Kryptographieverfahren erstellt. Hier wird ein Verfahren unter Verwendung

von elliptischen Kurven eingesetzt, da dieses bei relativ geringen Schlüssel- und Signaturlängen eine hohe Sicherheit sowie eine schnelle Verarbeitung bietet.

Eine gültige elektronische Signatur kann nur unter Verwendung eines so genannten privaten Schlüssels erzeugt werden. Dieser Schlüssel ist in gesicherter Form auf dem TIM gespeichert und damit nicht zugänglich. Die Echtheit der Signatur kann jedoch sehr einfach mit dem so genannten, zu einem privaten Schüssel gehörenden, öffentlichen Schlüssel überprüft werden. Der freie Zugriff auf den öffentlichen Schlüssel stellt kein Sicherheitsrisiko dar, da sich der private nicht aus dem öffentlichen Schlüssel herleiten lässt. Somit kann kein Unbefugter gültige Signaturen generieren.

Um sicherzustellen, dass der öffentliche Schlüssel tatsächlich zu dem privaten Schlüssel gehört (einem Prüfer also kein falscher Schlüssel „untergeschoben“ wurde), die Smartcard nicht als gestohlen gemeldet wurde usw. werden so genannte Zertifikate eingesetzt. Das sind strukturierte Daten, die den Eigentümer sowie weitere Eigenschaften des öffentlichen Schlüssels bestätigen. Das erfolgt im Wesentlichen dadurch, dass ein Zertifikat von einer vertrauenswürdigen Stelle wiederum digital signiert wird. Zudem wird ein zentrales Verzeichnis aller gesperrten Karten vorgehalten.

Durch ein Zertifikat können Nutzer des Systems einen öffentlichen Schlüssel einer Identität (z. B. einer Person, einer Organisation oder einem IT-System – in diesem Fall einem Unternehmen) zuordnen und seinen Geltungsbereich bestimmen. Damit ermöglichen digitale Zertifikate den Schutz der Vertraulichkeit, Authentizität und Integrität von Daten durch die korrekte Anwendung der öffentlichen Schlüssel. Die Verwaltung von Zertifikaten ist die Aufgabe einer so genannten „Public Key Infrastructure“ (PKI). Dabei handelt es sich um ein gängiges Verfahren in modernen Sicherheitsanwendungen.

### 2.2.3 Prüfabläufe

Die Prüfung von Daten, die von einem INSIKA-basierten System erzeugt wurden, unterscheidet sich deutlich von herkömmlichen Systemen.

Wesentlich ist die Tatsache, dass die Speicherung der Umsatzdaten exakt standardisiert ist. Das ist Grundvoraussetzung für eine herstellerunabhängige digitale Signatur und führt außerdem dazu, dass die Prüfung der Daten für alle INSIKA-konformen Systeme vollkommen identisch abläuft. Das standardisierte Datenformat bildet die bereits bestehenden Vorschriften zur Speicherung von Buchungsdaten (vor allem die GoBS = „Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme“ und die GDPdU = „Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen“) ab und kann daher von jedem System, das diese Vorschriften erfüllt, grundsätzlich erzeugt werden.

Die Prüfung, ob die Daten vollständig und unverändert sind, erfolgt vollautomatisch anhand der Signaturen und den Sequenznummern.

Mit diesen geprüften Daten ist die Plausibilisierung aller daraus abgeleiteten Daten (z.B. Tageseinnahmen, Abverkäufe bestimmter Produkte über beliebige Zeiträume) möglich. Die INSIKA-Buchungsdaten sind auswertbar, ohne auf weitere Daten (z.B. Stammdaten) zurückgreifen zu müssen. Bei Bedarf ist eine detaillierte Analyse der Rohdaten möglich, die Prüftiefe kann also dem jeweiligen Einzelfall angepasst werden.

In der Praxis wird die Prüfung voraussichtlich am besten in Form eines Import-Moduls für die von den Betriebsprüfern verwendete Software implementiert (in Deutschland ist das IDEA). Damit lässt sie sich nahtlos in bestehende Anwendungen und Abläufe integrieren.

Im Gegensatz zur momentanen Prüfungspraxis können Analysen zur Erkennung von Manipulationen (Benford-Analyse, Abgleich Verkaufsdaten einzelner Produkte entsprechenden Einkaufsmengen usw.) erheblich reduziert werden.

Fehlen die Daten trotz der Aufzeichnungspflicht oder sind sie unvollständig, ist eine Berechnung der Umsätze für die fehlenden Bereich aufgrund der sog. Tagesabschlüsse und der auf dem TIM geführten Summenspeicher möglich.

## 2.3 Unterschiede zu klassischen Fiskalspeichern

Im Gegensatz zu „klassischen“ Fiskalspeicherlösungen, wie sie z.B. in Italien oder diversen südamerikanischen und osteuropäischen Staaten eingesetzt werden, basiert die Sicherheit des INSIKA-Systems ausschließlich auf kryptografischen Verfahren.

Sobald ein korrekt signierter Beleg ausgegeben wird, ist die korrekte Funktionsweise des Systems nachgewiesen. Die Speicherung der Daten muss nicht besonders abgesichert werden. Da auch sonst keine Einschränkungen der Kassenfunktionen nötig sind, um die Sicherheit zu gewährleisten, ist keine Bauartzulassung, Zertifizierung o.ä. der Kassen erforderlich. Diese Schritte führen bei klassischen Fiskalspeichersystemen zu hohen Kosten, Wettbewerbsverzerrungen und einer Verzögerung oder gar Verhinderung technischer Weiterentwicklungen.

## 2.4 Sicherheit

Zur Bewertung der Sicherheit des Systems sollen im Folgenden die wesentlichen Teilaspekte betrachtet werden. Ausführlich werden diese Fragen in der Sicherheitsanalyse betrachtet, die im Rahmen des Projektes erstellt wird.

### 2.4.1 Kryptografie

Die Technik der elektronischen Signaturen ist ausgereift, sehr sicher und wird heute vielfach eingesetzt, z.B. im Bankensektor oder bei der elektronischen Steuererklärung.

Um möglichst kurze Signaturen zu erhalten und die Verarbeitungszeiten zu minimieren, wurden im INSIKA-Projekt Signaturen auf Basis elliptischer Kurven ausgewählt (ECC = „Elliptic Curve Cryptography“ bzw. ECDSA = „Elliptic Curve Digital Signature Algorithm“). Als Schlüssellänge werden 192 Bit verwendet, was nach dem aktuellen Wissenstand eine ausreichende Sicherheit auch in der Zukunft gewährleistet. Die Architektur sieht jedoch die Möglichkeit vor, bei Bedarf längere Signaturen einsetzen zu können.

Zum Nachweis der Vollständigkeit und Unversehrtheit der Buchungsdaten wird eine kryptografische Hash-Funktion (gewissermaßen der „Fingerabdruck“ der Buchungsdetails) verwendet.

Wesentlich bei sicheren kryptografischen Verfahren ist, dass die Sicherheit nicht von der Geheimhaltung des Verfahrens selbst abhängt, sondern von der Geheimhaltung der privaten Schlüssel. Die Verfahren werden vielmehr veröffentlicht und unterliegen damit einer ständigen Überprüfung durch Fachleute.

### 2.4.2 Smartcards

Das INSIKA-System sieht den Einsatz handelsüblicher, evaluierter Smartcards mit einer zusätzlichen Sicherheitssoftware vor. Darüber hinaus sind die Karten mit einer Software gemäß der INSIKA-Spezifikation versehen.

Die Hardware und Systemsoftware der Karten ist gegen alle bekannten Angriffe nach dem Stand der Technik abgesichert.

Durch den Einsatz neuerer Generationen von Smartcards im Laufe des Betriebs ist - falls erforderlich - eine Erhöhung des Sicherheitsniveaus möglich.

### 2.4.3 Verknüpfung karteninterner Abläufe

Wesentlich für die Sicherheit ist die feste Verknüpfung karteninterner Funktionen untereinander und mit Vorgängen in der Kasse. Das sind im Einzelnen:

- Sequenzzähler: Der Sequenzzähler, der alle Buchungen fortlaufend nummeriert, wird vom TIM verwaltet und von diesem direkt in die Signaturberechnung einbezogen. Dadurch sind Manipulationen an dieser Stelle grundsätzlich ausgeschlossen. Eine Veränderung des Zählers von außen ist nicht möglich.
- Plausibilitätsprüfungen im TIM: Wesentliche Zusammenhänge einzelner Beträge (Steuerberechnung und Plausibilität des Ausweises von Negativumsätzen) werden vom TIM vor der Signaturberechnung überprüft. Sind die Daten nicht plausibel, wird keine Signatur geliefert.
- Summenzähler: Exakt festgelegte Daten werden im TIM monatsweise in Summenform gespeichert (z.B. Gesamtumsatz und Umsatzsteuer getrennt nach Steuersätzen). Sollten die Buchungsdaten (deren Aufbewahrung verpflichtend ist) nicht mehr vorhanden, unvollständig oder fehlerhaft sein, stehen immer noch die Summendaten zur Verfügung und erlauben, die Lücken in den Daten zu schließen. Die Aktualisierung der Zähler erfolgt immer zusammen mit der Signaturerstellung und kann daher nicht manipuliert werden.

### 2.4.4 Korrekte Nutzung des Systems

Wie bei jedem fiskalisierten oder nicht fiskalisierten Kassensystem ist die korrekte Erfassung **aller** Buchungen eine entscheidende Grundanforderung**.**

Dies wird im INSIKA-Konzept und dem zugrundeliegenden Gesetzentwurf vom Juli 2008 durch folgende Maßnahmen sichergestellt:

- Verpflichtung zum Einsatz des INSIKA-Systems in jeder Registrierkasse
- Verpflichtung, zu jedem Verkaufsvorgang einen gedruckten Beleg mit einer darauf gedruckten, gültigen Signatur auszugeben. Der Beleg muss alle Daten enthalten, um damit die Signatur ohne Zugriff auf weitere Daten (die z.B. in der Registrierkasse gespeichert werden) verifizieren zu können
- Unangekündigte Kontrollen, die eine Einhaltung der Verpflichtungen sicherstellen (im Rahmen der sog. „Kassennachschau“)

Grundsätzlich kann die technische Seite der Lösung sicherstellen, dass die Nicht- oder die fehlerhafte Nutzung des Systems einfach und zuverlässig erkannt werden kann. Über eine entsprechende Überwachung muss dann das Entdeckungsrisiko groß genug sein, dass Betrug entweder verhindert oder ausreichend wahrscheinlich erkannt wird.

## 2.5 Kostenbetrachtung

Aus der Erfahrung der bisherigen Projektarbeit lässt sich ableiten, dass für die Integration der INSIKA-Lösung in ein bestehendes Kassensystem mit einem Entwicklungsaufwand von etwa ein bis fünf Mann-Monaten zu rechnen ist. Dieser Aufwand ist stark von der technischen Ausgangssituation abhängig.

Die Materialkosten für einen Kartenleser (extern oder intern) liegen im niedrigen zweistelligen Bereich. Die Integration eines Kartenlesers bedingt einen nicht allgemein zu beziffernden Einmalaufwand (es können z.B. Änderungen an Elektronikbaugruppen und evtl. an Gehäuseteilen erforderlich sein).

Bei einer Gesamtbetrachtung sind folgende Aspekte zu berücksichtigen:

- In vielen Fällen wird die Nachrüstung bestehender Systeme aus dem Anschluss eines Kartenlesers und einer Aktualisierung der Kassensoftware bestehen.
- Während der Übergangsfrist (also der Frist zwischen Inkrafttreten einer entsprechenden Verordnung und der Pflicht zur Benutzung des Systems) werden viele Systeme ohnehin regulär ausgetauscht bzw. gewartet, so dass hier keine nennenswerten Zusatzkosten entstehen.
- Durch die vergleichsweise einfache Implementierung des INSIKA-Systems wird sich die Wettbewerbsintensität nicht verringern, so dass dieser Faktor kostendämpfend wirken wird.

Nach den Analysen ist das INSIKA-System ganz erheblich preiswerter in Entwicklung, Einführung und Betrieb als alle bisher bekannten Fiskalsysteme bei gleichzeitiger Erhöhung der Sicherheit.

# 3 INSIKA-Demonstrator

## 3.1 Aktueller Stand der Entwicklung

Die gesamte Demonstrationssoftware befindet sich in einem Erprobungsstadium, so das konzeptionelle und Implementierungsfehler nicht auszuschließen sind.

Speziell der Kassensimulator und die Verifikationssoftware (IVM) haben ausdrücklich den Charakter einer Demonstrationssoftware. Beide Programme wurden von der PTB im Rahmen des INSIKA-Projektes entwickelt.

Bei der Software des TIM handelt es sich um einen Prototypen, der bereits sorgfältig getestet wurde. Fehler sind aber auch hier nicht auszuschließen.

## 3.2 Aufgaben der Software

Mit dem INSIKA-Softwarepaket kann die Funktion von INSIKA von der Erzeugung von signierten Kassendaten, über deren Speicherung und Umwandlung in das INSIKA-Exportformat bis zur Verifikation einschließlich des Zugriffs auf den INSIKA-Zertifkats-Testserver demonstriert werden. Dabei laufen die Prozesse ab, die in die realen INSIKA-Prototypkassen integriert sind.

## 3.3 Einrichtung

Alle drei Programme des INSIKA-Demonstrators sind ohne Installation der Software direkt auf einem PC lauffähig. Hinweise zur Verwendung befinden sich in jedem Softwarepaket.

## 3.4 Funktionen

### 3.4.1 Kassensimulator

Der Kassensimulator erlaubt dem Anwender auf einfache Weise, alle INSIKA-Funktionen einer Kasse zu testen. Dazu gehören das Aktivieren des TIM, Durchführen von Buchungen und Tagesabschlüssen. Es wird ein elektronisches Journal erzeugt, welches vom IVM verifiziert werden kann. Mit dem Kassensimulator kann ein breites Spektrum von Anwendungsfällen nachgebildet werden. Dazu gehören u.a. der Trainingmodus, Rückbuchungen, Artikel mit mehreren Umsatzsteuersätzen und der Umsatzsteuersatzwechsel. Auch können verschiedene Sonderfälle wie Lieferschein- und Agenturgeschäft abgebildet und die Reaktion des Gesamtsystems auf inkonsistente Zeitangaben getestet werden.

Um mit dem Kassensimulator arbeiten zu können, werden lediglich ein PC mit Windows XP (andere Betriebssysteme, insbesondere Windows Vista, wurden noch nicht getestet), ein Kartenleser, der von Windows XP unterstützt wird und installiert ist sowie ein personalisiertes TIM benötigt. Eine Installation der Software ist nicht notwendig. In dem sich öffnenden Standardfenster der Kasse können einzelne Buchungen durchgeführt werden. Dazu sind aus der Produktliste vorbereitete Produkte durch Mausklick oder über den Button „Hinzufügen“ auszuwählen. Die Kommunikation zwischen PC und TIM kann in verschiedenen Monitorfenstern verfolgt werden. Eine detaillierte Beschreibung ist in der Programmdokumentation < Kurzbeschreibung_Kass_Sim.pdf > zu finden.

### 3.4.2 IVM

Das Programm IVM (INSIKA Verification Module) ermöglicht die Überprüfung von signierten Buchungen und signierten Tagesabschlüssen sowie die Echtheitsprüfung von Belegen mit aufgedruckter Signatur. Buchungen müssen im INSIKA-XML-Exportformat bereitgestellt werden. Die zur Überprüfung erforderlichen Zertifikate werden entweder der XML-Datei entnommen oder vom INSIKA-Zertifikatsserver direkt gelesen. Im einfachsten Fall signalisiert das Programm über eine Farbinformation das Ergebnis der Prüfung – Grün – Prüfung erfolgreich, Rot – Prüfung fehlgeschlagen. Für den Online-Zugriff auf den INSIKA-Zertifikatsserver sind u.U. im Rechnernetz bestimmte Ports freizugeben. Eine detaillierte Beschreibung ist in der Programmdokumentation <Kurzbeschreibung IVM.pdf> zu finden.

### 3.4.3 TIM-Browser

Der TIM-Browser ist ein Programm zur Anzeige der INSIKA-relevanten Daten des TIM. Um das Programm benutzen zu können, muss ein Kartenleser installiert sein. Das Programm wurde unter Windows XP getestet. Eine Kurzbeschreibung ist in der Datei <Readme.txt> des Programmordners zu finden.

## 3.5 Verwendungsbeispiel

In diesem Abschnitt werden die wesentlichen Abläufe einer INSIKA-Demonstration unter Verwendung der beschriebenen Programme zusammenfassend dargestellt. Details können in den einzelnen Programmdokumentationen nachgeschlagen werden.

Um die Arbeitschritte Erzeugung von INSIKA konformen Daten und deren Überprüfung nachvollziehen zu können, werden der Kassensimulator und das IVM benötigt.

Nach dem Start des Kassensimulators können aus der Produktliste einzelne Artikel durch Mausklick ausgewählt und somit in eine Buchung aufgenommen werden. Über die Zwischenschritte ‚Summe' und ‚Kassieren' wird eine Transaktion der Daten zum TIM ausgelöst und die Buchung abgeschlossen. Das Ergebnis der Transaktion wird auf dem Beleg ausgegeben und im Journal des Kassensimulators als abgeschlossene Buchung gespeichert. Diese Kassiervorgänge können beliebig oft wiederholt werden.

Außerdem können Tagesabschlüsse erzeugt werden. Das entsprechende Fenster öffnet sich bei Betätigen des Buttons ‚Tagesabschluss öffnen'. Wird ein Tagesabschluss mit Signatur durchgeführt, so erscheint auch dieser auf dem Beleg und wird im Journal gespeichert.

Um die so entstandenen Daten überprüfen zu können, muss der Kassensimulator beendet werden. Erst danach können die im Unterverzeichnis „Journal" befindlichen Journale geöffnet werden. Die elektronischen Journale liegen im INSIKA-XML-Format sowohl im Format "Klartext" (Langform) als auch im Format "Base64" (Kurzform) vor. Diese Dateien können mit Hilfe des IVM überprüft werden.

Nach dem Start des IVM wählt man über ‚Datei(en) laden' die zu prüfenden Dateien aus (einzelne Datei oder Gruppe). Das Programm prüft die signierten Daten und stellt das Prüfergebnis dar („Verifikation erfolgreich" – grün oder „mindestens eine Verifikation fehlerhaft" – rot). Bei entsprechender Ansicht werden weitere Details der geprüften Dateien dargestellt.

Der TIM-Browser erlaubt es dem Anwender auf einfache Art und Weise zu zeigen, welche Daten direkt auf dem TIM gespeichert werden. Außerdem kann für Prüfzwecke mit diesem Programm das Zertifikat direkt vom TIM ausgelesen werden.

# 4 Implementierung in Kassensysteme

In diesem Abschnitt wird ein allgemeiner Überblick über die Implementierung des INSIKA-Systems in Kassensysteme gegeben. Damit soll der Leser in die Lage versetzt werden, Ablauf und Aufwand einer Implementierung schnell abschätzen zu können. Auch das Verständnis der TIM-Spezifikation soll hiermit erleichtert werden.

## 4.1 Voraussetzungen

Ein Kassensystem muss einige Voraussetzungen erfüllen, um eine INSIKA-Implementierung zu ermöglichen:

- Die Ansteuerung einer Smartcard über einen externen oder eingebauten Kartenleser muss möglich sein
- Ein Drucker für alphanumerische Zeichen muss vorhanden sein
- Das INSIKA-System ist im Wesentlichen durch zwei Schnittstellen definiert: die TIM-Signaturschnittstelle und die XML-Exportschnittstelle. Die TIM-Signaturschnittstelle ist im Dokument "INSIKA_TIM_Schnittstelle-[version]" spezifiziert. Die XML-Exportschnittstelle ist im Dokument "INSIKA_XML_Export-[version]" festgelegt. Ein Kassensystem muss beide Schnittstellen bedienen. Die XML-Exportschnittstelle kann dabei auch durch ein nachgelagertes System (z.B. PC) bedient werden.
- Ein INSIKA-Kassensystem muss ein Journal führen, in dem jede Buchung und jeder Tagesabschluss abgelegt werden. Die Größe, das Format und die Implementierung sind jedem Hersteller selbst überlassen. Einzige Bedingung ist, dass die Buchungen und Tagesabschlüsse vollständig in das festgelegte XML-Format gewandelt werden können. Nur so ist die Prüfung der Daten – speziell die Signaturverifikation – möglich. Es müssen ausreichend Speicherkapazität sowie die passenden Verwaltungsmechanismen für das Journal vorhanden sein. Ein eventuell vorhandenes elektronisches Journal muss zumindest um die Speicherung von Sequenznummer und Signatur ergänzt werden. Das Journal muss auf ein Computersystem, z.B. einen PC übertragbar sein (z.B. über serielle-, Netzwerk- oder USB-Schnittstellen, Datenträger wie z.B. USB-Sticks, SD-Karten oder über Internet-Protokolle)

## 4.2 Ansteuerung des TIM

Das TIM ist eine handelsübliche Smartcard, die ein Betriebssystem und ein spezielles TIM-Package enthält. Die TIM-Signaturschnittstelle ist durch den Standard ISO/IEC 7816 Teil 1-4 in der physikalischen Schicht, sowie in der Sicherungs- und Anwendungsschicht definiert. Die für INSIKA nötigen Erweiterungen auf Ebene der Anwendungsschicht sind im Dokument "INSIKA_TIM_Schnittstelle-[version]" spezifiziert.

Das TIM wird im Format ID-1 ausgeliefert (Kreditkartengröße). Die Smart Card ist so perforiert, dass sie sich durch einfaches Ausbrechen in das ID-000 Format (SIM-Kartengröße) verwandeln lässt.

Die Ansteuerung des TIM kann mit jedem handelsüblichen Kartenleser durchgeführt werden. Ein Kartenleser der Klasse 1 ist dabei vollkommen ausreichend, ein PIN-Pad ist nicht not-

wendig. Der Kartenleser muss lediglich das „T=1“-Protokoll entsprechend der ISO/IEC 7816 unterstützen. Die zur erstmaligen Aktivierung erforderliche Transport-PIN wird mit den Schnittstellen-Befehlen vom Host an das TIM übertragen. Nutzbar ist dazu z.B. der Kassensimulator.

Für viele Kassensysteme ist ein feste Integration des Kartenlesers und des TIM sinnvoll. Für die Ansteuerung des ISO/IEC 7816 Interfaces lassen sich dafür unterschiedliche ICs nutzen. Einige ICs bieten dabei neben der physikalischen Schnittstelle zur Smart Card auch Controller, die bereits einen "T=1" Protokollstack mitbringen. Da die Ansteuerung von Smart Cards standardisiert ist, wird diese hier nicht weiter ausgeführt. Einen Überblick zu Smart Cards bietet z.B. das "Handbuch der Chipkarten" von W. Rankl und W. Effing.

Es ist zu beachten, dass die Geschwindigkeit der Kommunikation mit dem TIM vom Kartenleser und der Treibersoftware abhängen. Ist die Kommunikation optimal implementiert, wird die Zeit für einen INSIKA-Buchungsvorgang praktisch nur durch die Signaturberechnung selbst bestimmt. Mit den momentan verwendeten Smartcards dauert ein Buchungsvorgang etwa 300 ms und führt bei einer sauberen Implementierung nicht zu störenden Verzögerungen.

Die Kommunikation mit Smartcards ist weitgehend normiert, so dass für viele Systeme geeignete Bibliotheken zur Verfügung stehen. Muss die Kommunikation neu implementiert werden, ist vor allem die Erzeugung und Auswertung von TLV-Datenobjekten zu entwickeln. TLV steht für „Tag-Length-Value“ – ein Datenobjekt wird dabei durch einen Bezeichner, die Länge und den eigentlichen Dateninhalt kodiert.

Die Kommunikation besteht immer aus einer Command-APDU („Application Protocol Data Unit“), die vom Host-System (also der Registrierkasse) an das TIM als Request gesendet wird. Je nach Befehl antwortet das TIM darauf mit einem entsprechenden Response und einem Result-Code.

## 4.3 Datenaufbereitung, Einbindung TIM

Beim Abschluss jeder Buchung müssen folgende Schritte durchgeführt werden:

- Aufbereitung der Daten des Belegs (inkl. Errechnen des Positions-Hashwertes, dazu müssen die Belegpositionen in ein genau definiertes Format umgewandelt werden und über diese Daten ein SHA-1-Hashwert errechnet werden)
- Einige besondere Details der Buchung müssen ausgewiesen werden:
  - Agenturumsatz: Umsätze, die im Namen Dritter getätigt werden, z.B. ist der Kraftstoffverkauf bei den meisten Tankstellen ein Agenturgeschäft
  - Lieferscheine: Umsätze, die auf dem Beleg ausgewiesen werden, später jedoch über ein anderes System (z.B. zentrale Rechnungsstellung) aber vom gleichen Unternehmen fakturiert werden
  - Trainingsbuchungen: Buchungen, die zu Test- oder Ausbildungszwecken durchgeführt werden
- Alle ermittelten Daten sind im passenden Format an das TIM zu übertragen
- Die Rückmeldungen des TIM (zumindest die Sequenznummer und die Signatur) müssen gespeichert und zusammen mit den anderen Daten auf dem Beleg gedruckt werden

- Tritt ein Fehler auf, muss eine entsprechende Fehlerbehandlung durchgeführt werden (Fehlermeldung, wenn sinnvoll Wiederholung der Kommunikation)

## 4.4 Druck verifizierbarer Belege

Ein wesentliches Element des INSIKA-Systems ist die Verifizierbarkeit von gedruckten Belegen, ohne dabei auf andere aufgezeichnete Daten zurückgreifen zu müssen.

Daher müssen die Belege alle Daten, die in die Signatur einfließen, vollständig enthalten. Dies ist aufgrund der rechtlichen Anforderungen allerdings auch ohne eine INSIKA-Implementierung der Fall.

Weitere Informationen zum Belegdruck enthält das Dokument "INSIKA_XML_Export-[version]".

## 4.5 Speicherung Buchungsjournal

Alle Buchungen müssen mit den dazugehörigen Sequenznummern und Signaturen gespeichert werden.

Die einzige inhaltliche Anforderung an die Speicherung der Daten ist, dass sie im definierten XML-Format exportiert werden müssen. Es ist möglich und in vielen Fällen sicher auch technisch sinnvoll, nicht das XML-Format, sondern ein optimiertes Format zur internen Speicherung der Daten zu verwenden und das XML-Format erst beim Export zu erzeugen.

Die Speicherung der Daten kann durchaus über längere Zeiträume in der Kasse erfolgen. Es ist aber auch möglich, die Daten z.B. täglich oder wöchentlich auf ein System mit höherer Speicherkapazität (z.B. einen PC) zu übertragen.

Nach bisherigen Tests ist bei einer optimierten Speicherung mit einem Datenaufkommen (für das gesamte Buchungsjournal) von weniger als 50 kByte pro Tag (bei 200 Verkaufsvorgängen mit je 3 Positionen) bis ca. 600 kByte pro Tag (bei 1.000 Vorgängen mit je 20 Positionen) auszugehen.

In jedem Fall ist zu beachten, dass eine regelmäßige Datensicherung erfolgt (analog zu allen anderen steuerlich relevanten, digital gespeicherten Daten).

## 4.6 Tagesabschlüsse

Täglich muss ein signierter Tagesabschluss durchgeführt werden. Dabei werden Gesamtsummen aller Umsätze, die bisher vom TIM erfasst wurden, vom TIM in signierter Form an die Kasse geliefert. Sie müssen im Buchungsjournal gespeichert werden. Es bietet sich an, diesen Tagesabschluss in eine bereits bestehende Kassenabrechnungsfunktion zu integrieren.

Diese Tagesabschlüsse beschleunigen die Verifikation von Buchungsdaten, da durch sie in vielen Fällen auf die Signaturprüfung jeder einzelnen Buchung verzichtet werden kann.

Sie helfen ferner dabei, Umsätze für Perioden zu errechnen, für die keine Umsatzdaten vorliegen.

## 4.7 Verarbeitung Buchungsjournal

Speziell bei Filialbetrieben können relativ große Datenmengen anfallen. Beim Datenzugriff im Rahmen einer Betriebsprüfung müssen die Buchungen fortlaufend pro TIM bereitgestellt werden.

Je nach den organisatorischen Gegebenheiten (z.B. Einsatz von Kassen an verschiedenen Orten, evtl. Einsatz von Austauschgeräten bei Reparaturen usw.) ist eine entsprechende Aufbereitung der Buchungsdaten erforderlich. Diese Anforderungen sind jedoch nicht durch das INSIKA-System bedingt, sondern resultieren bereits aus den GoBS und GDPdU und sollten bereits Bestandteil typischer Backoffice-Software sein.

## 4.8 XML-Export Buchungsjournal

Wie bereits beschrieben, müssen alle Buchungsdaten in einem exakt definierten XML-Format bereitgestellt werden.

Um den Speicherplatzbedarf und die Verarbeitungsgeschwindigkeit zu optimieren, kann mit einem systemspezifischen Format gearbeitet werden und das XML-Format erst beim Export erzeugen werden.

Die XML-Exportschnittstelle ist im Dokument "INSIKA_XML_Export-xx" festgelegt. Darin wird das XML-Schema dargelegt, das den Aufbau und den Inhalt der XML-Dokumente vorgibt. Um das INSIKA-System zu schließen, müssen sich aus dem XML-Dokument die ursprünglich vom TIM signierten Daten zurückgewinnen lassen. Nur so lässt sich eine Signaturverifikation durchführen.

In den Exportdaten müssen sich zudem die vom TIM vergebenen Sequenznummern für jede Buchung wieder finden lassen. Die Konsistenz dieser Sequenznummern stellt die Vollständigkeit der Daten sicher.

## 4.9 Hilfsfunktionen

Folgende zusätzliche Hilfsfunktionen sind für die korrekte Funktion des Systems erforderlich:

- Aktivierung: Ein neues TIM muss einmalig mit Hilfe einer Transport-PIN aktiviert werden, um einen Missbrauch von TIMs zu vermeiden (z.B. wenn sie auf dem Postweg zum Anwender gestohlen wurden).
- Deaktivierung: Ein TIM ist nur ein bestimmte Zeit einsetzbar (z. Zt. sind 10 Jahre vorgesehen). Nach Ablauf dieser Zeit sollte die Karte mit dem entsprechenden Befehl deaktiviert werden. Dies macht die Erstellung weiterer Buchungssignaturen unmöglich. Die signierte Rückmeldung des TIM erlaubt den eindeutigen Nachweis der Deaktivierung, ohne dass dazu ein physischer Zugriff auf die Karte erforderlich ist.
- Zertifikat lesen: Die XML-Exportdatei muss ein Zertifikat für jedes verwendete TIM enthalten. Aus Sicht der Kasse handelt es sich lediglich um einen Datensatz, der einmalig aus dem TIM gelesen, zwischengespeichert und exportiert werden muss.

Die folgenden Funktionen machen die Arbeit mit Systemen komfortabler:

- Weitere Berichte: Neben dem bereits erwähnten Tagesabschluss lassen sich Berichte für frei wählbare Zeiträume auslesen. Der Anwender kann damit selbst kontrollieren, in welcher Höhe Umsätze durch das TIM signiert wurden.
- Verzeichnis der Karten: Sobald eine größere Menge von TIMs eingesetzt wird (typischerweise in Filialbetrieben) sind Funktionen zur zentralen Verwaltung der TIMs sinnvoll, damit der Anwender jederzeit einen Überblick über die aktuelle Situation hat (z.B.: Welche TIMs sind seit wann in welchem Kassenplatz eingesetzt?).
- Eigene Verifikation: Um sicherzustellen, dass die für eine Prüfung bereitgestellten Daten korrekt sind (und nicht z.B. aufgrund eines Bedienungsfehlers eine Lücke in den Sequenznummern aufweisen) sollte es eine Prüfungsroutine für diese Daten geben. Aufgrund des herstellerunabhängigen XML-Formats und des offenen und auf Standards basierenden INSIKA-Verfahrens ist es möglich, eigene Verifikationssoftware zu entwickeln.

Alle beschriebenen Funktionen können an der Kasse oder auch in einem separaten PC-System implementiert werden. Letzteres bietet sich vor allem bei Filialbetrieben an, um das gesamten Handling der TIMs zu zentralisieren.