INSIKA®: Kryptografischer Manipulationsschutz für Registrierkassen und Taxameter

Stand: August 2014

INSIKA-Projekt

Die Abkürzung INSIKA steht für „**IN**tegrierte **SI**cherheitslösung für messwertverarbeitende **KA**ssensysteme“. Diese Lösung wurde in einem Projekt unter Leitung der Physikalisch-Technischen Bundesanstalt (PTB) zur Serienreife entwickelt.

Die Anwendung des INSIKA-Konzepts stellt die lückenlose, revisionssichere Aufzeichnung von Einzelbuchungen bei Bargeschäften unter Nutzung einer elektronischen Registrierkasse (oder vergleichbarer Komponenten wie z. B. Taxameter) 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. Alle mit Hilfe der Smartcard erzeugten Daten werden zusammen mit den Daten der Buchung in ein Standardformat gewandelt.

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.

Auslöser für das INSIKA-Projekt war das auf Veranlassung des Bundesrechnungshofes (BRH) vom Bundesministerium der Finanzen (BMF) in zwei Bund-Länder-Arbeitsgruppen erarbeitete Fachkonzept für die Absicherung der in Registrierkassen und Taxametern erzeugten Daten gegen Manipulationen. Die Physikalisch-Technische Bundesanstalt (PTB) entwickelte zusammen mit mehreren Partnern aus der Industrie die dafür erforderliche technische Lösung.

Das Projekt wurde im Februar 2012 erfolgreich abgeschlossen.

Funktionsprinzip

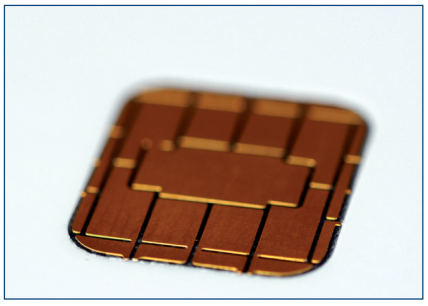
Der Manipulationsschutz basiert auf einer digitalen Signatur, die von einer durch eine autorisierte zentrale Stelle ausgegebenen Smartcard erzeugt wird. Damit ist eine Prüfung der korrekten Erfassung der Daten jederzeit möglich. Die mit der Signatur geschützten Daten können nicht unerkannt verändert werden. Selbst bei einer Manipulation oder beim Verlust der Daten ist durch technische Vorkehrungen eine Ermittlung der einmal signierten Gesamtumsätze möglich.

Die Lösung basiert auf bewährter, moderner Sicherheitstechnik. Sie ist vergleichsweise einfach zu implementieren und erfordert keine wesentlichen technischen Auflagen für Registrierkassen bzw. Taxameter und in Folge auch keine Bauartzulassung oder Zertifizierung. Damit ist sie klassischen Fiskalspeicherlösungen in jeder Hinsicht deutlich überlegen.

Das Gesamtkonzept und die Spezifikation aller Schnittstellen sind vollständig offengelegt.

Technik im Detail

INSIKA-Smartcard



Um eine Registrierkasse oder ein Taxameter abzusichern, werden handelsübliche Smartcards verwendet, die jedoch mit einer speziellen Software ausgestattet sind. Diese sollen bei gesetzlich vorgeschriebener Umsetzung von der Finanzverwaltung in einem offenen Ausschreibungsverfahren beschafft und an Steuerpflichtige auf Antrag ausgegeben werden. Dies kann durch die Behörden selbst, aber auch durch von ihnen beauftragte private, anerkannte Dienstleister erfolgen.

Die Smartcard kann über einen externen Kartenleser angeschlossen oder (wie z. B. bei Mobiltelefonen) in das Gerät integriert werden. Die Software der Registrierkasse bzw. des Taxameters muss die Smartcard entsprechend ansteuern und den

Ausdruck sowie die Speicherung der Daten gewährleisten. Darüber hinausgehende Änderungen an Registrierkasse bzw. Taxameter sind nicht erforderlich. Ein großer Teil der am Markt befindlichen Registrierkassen und Taxameter kann ohne großen Aufwand nachgerüstet werden.

Digitale Signaturen

Ein wesentliches Element der Lösung ist der Einsatz digitaler Signaturen. Mit digitalen Signaturen lässt sich sicher feststellen, dass Daten von einer bestimmten Person oder einem System (hier: einer ganz bestimmten Registrierkasse bzw. einem Taxameter) stammen und dass die Daten seit Erstellung der Signatur nicht verändert wurden. Die Technik der digitalen Signaturen ist ausgereift, sehr sicher und wird heute vielfach eingesetzt, z. B. im Bankensektor oder bei der elektronischen Steuererklärung. In den meisten Anwendungsfällen mit hohen Sicherheitsanforderungen – wie auch im INSIKA-System – werden Smartcards zur Erzeugung der Signaturen eingesetzt.

Kassenbelege mit Signatur

Gedruckte Kassenbelege und die zugehörigen, elektronisch gespeicherten Buchungen werden mit einer digitalen Signatur versehen. Diese Signatur wird von der Smartcard berechnet. Ferner führt die Smartcard einen internen Zähler, mit dem für jede Buchung und den dazugehörigen gedruckten Beleg eine eindeutige und fortlaufende Nummer vergeben wird. Zusätzlich werden in der Smartcard Summenspeicher verwaltet. Diese erfassen die Gesamtumsätze so, 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 in der Smartcard so miteinander verknüpft, dass die Erzeugung einer Signatur für den Ausdruck gleichzeitig die Vergabe einer neuen Sequenznummer und Aktualisierung der Summenspeicher auslöst.

Über einen Zwang zur Ausgabe von Belegen mit gültigen Signaturen ist somit die korrekte Aufzeichnung der Daten sichergestellt, da alle weiteren Schritte über Verknüpfung der verschiedenen Funktionen innerhalb der Smartcard erzwungen werden.

Manipulationen von Kassendaten

Weltweit werden in vielen Branchen mit hohem Barzahlungsanteil Umsätze verkürzt und damit Steuern sowie Sozialleistungen hinterzogen. Da aus betrieblichen Gründen trotzdem eine Erfassung an der Registrierkasse erforderlich ist, ergibt sich daraus der Bedarf, die Daten zu manipulieren. So eine Manipulation kann entweder während der Erfassung (z. B. indem Daten teilweise nicht in die Kasse eingegeben werden oder durch Softwarefunktionen, die Daten manipuliert abspeichern) oder nachgelagert (durch Veränderungen an bereits abgespeicherten Daten, z. B. durch sogenannte „Zapper"-Software) erfolgen.

Zur Vermeidung von Manipulationen muss zum einen eine stichprobenartige Kontrolle der korrekten Erfassung möglich sein und zum anderen verhindert werden, dass die Daten nach der Erfassung unerkannt verändert werden können.

Es wird versucht, diese Ziele entweder über technische Ansätze (konventionelle Fiskalkassen oder INSIKA) oder lediglich durch verschärfte Prüfungen zu erreichen. Um entsprechende Prüfungen zu erleichtern, verlangen immer mehr Finanzbehörden die Aufzeichnung von Einzeltransaktionen statt summierter Werte. In Deutschland ist das durch das BMF-Schreiben vom 26.11.2010 geschehen. Bei geschickter Manipulation der Transaktionsdaten – vor allem durch „Zapper"-Software, die entsprechende Veränderungen automatisch ausführt – sind die Veränderungen jedoch auch mit modernen Analysemethoden nicht aufzudecken.

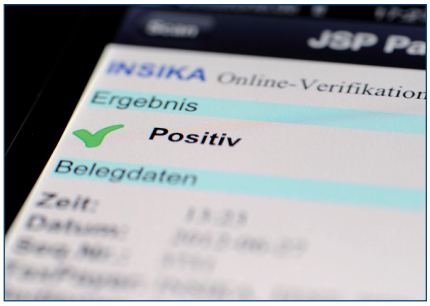
Beim Einsatz in Taxametern wurde statt der Belegerstellung eine Online-Datenübertragung als Kontrollmöglichkeit vorgesehen. Hier erfolgt die Überprüfung der korrekten Nutzung des Systems über die Prüfung der Transaktionsdaten auf einem Server und nicht über gedruckte Belege.

Prüfung von Kassenbelegen und Kassendaten

Für die INSIKA-Lösung werden im Wesentlichen nur Transaktionsdaten gespeichert, zu deren Aufbewahrung Steuerpflichtige spätestens aufgrund des BMF-Schreibens vom 26.11.2010 ohnehin bereits verpflichtet sind. Neu ist dabei nur die Signatur. Über sogenannte Profile ist eine Anpassung auf verschiedene Arten von zu speichernden Daten möglich – momentan existieren Profile für Registrierkassen und Taxameter.

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. Selbst durch bewusst in eine Registrierkasse integrierte Manipulationsfunktionen kann das System nicht angegriffen werden. Daher ist eine aufwändige Zertifizierung der Geräte überflüssig. Die Prüfung der aufgezeichneten Daten kann in weiten Teilen automatisiert werden und ist damit wesentlich effizienter als in der Vergangenheit. Es wird ein standardisiertes XML-Format verwendet, was eine sichere Prüfung der Signaturen erlaubt und alle Unsicherheiten in Bezug auf Form und Inhalt beseitigt.



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 gültiger Smartcard erstellt wurde. Jede falsch erstellte Rechnung ohne oder mit ungültiger Signatur stellt einen eindeutigen Beweis für eine Manipulation dar. Mit einem 2D-Code auf dem Ausdruck kann die Prüfung eines Belegs sogar praktisch vollautomatisch erfolgen.

Im Unterschied zur aktuellen rechtlichen und technischen Situation kann ein Steuerpflichtiger die Korrektheit seiner Daten erstmalig beweisen.

Kosten und Auswirkungen auf den Markt

Klassische Fiskalspeicherlösungen basieren auf einem mechanischen Schutz eines Speichers für die zu schützenden Daten, der Geheimhaltung von technischen Details und auf einer Reihe komplexer Auflagen für die Funktionsweise der Registrierkassen. Die Einhaltung der Vorschriften wird in einem Zertifizierungsverfahren geprüft. Dieser Ansatz macht solche Systeme teuer, reduziert den Funktionsumfang und verhindert technische Weiterentwicklungen (da jede Änderung eine Neuzertifizierung erfordert). Eine Kontrolle der korrekten Nutzung ist schwierig, da die Belege keinerlei Sicherheitsmerkmale aufweisen. Gleichzeitig entspricht das Sicherheitsniveau nicht mehr heutigen Standards.

In den letzten Jahren sind die klassischen Fiskalsysteme teilweise mit kryptografischen Funktionen ergänzt, aber dabei nicht neu konzipiert worden (z. B. in Schweden und Belgien). So sind komplexe Lösungen entstanden, die aber nicht die elementaren Nachteile beseitigen, sondern vor allem Aufwand und Kosten erhöhen.

Digitale Signaturen

Für INSIKA geeignete digitale Signaturen werden mit asymmetrischen Kryptografieverfahren erstellt. Bei INSIKA wird ein System unter Verwendung von elliptischen Kurven eingesetzt (ECDSA), da dieses bei relativ geringen Schlüssel- und Signaturlängen eine hohe Sicherheit bietet und eine schnelle Berechnung erlaubt.

Eine gültige digitale Signatur kann nur unter Verwendung eines sogenannten privaten Schlüssels erzeugt werden. Dieser Schlüssel ist in gesicherter Form, i. d. R. auf einer Smartcard gespeichert und damit nicht zugänglich. Die Echtheit der Signatur kann jedoch sehr einfach mit einem sogenannten 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. Selbst wenn ein einzelner Schlüssel „geknackt" würde, ist die Sicherheit aller anderen Systeme nicht gefährdet.

Um sicherzustellen, dass der öffentliche Schlüssel tatsächlich zu dem privaten Schlüssel gehört, die Smartcard nicht als verloren oder gestohlen gemeldet wurde usw. werden sogenannte Zertifikate eingesetzt. Ein Zertifikat ist ein Datensatz, der den Eigentümer sowie weitere Eigenschaften sicher und nachprüfbar mit dem öffentlichen Schlüssel verknüpft. Durch ein Zertifikat können Nutzer des Systems einen öffentlichen Schlüssel einer Identität (z. B. einer Person, einer Organisation oder einem IT-System) zuordnen und seinen Geltungsbereich bestimmen. Damit ermöglichen digitale Zertifikate den Schutz der Authentizität und Integrität von Daten. Die Verwaltung von Zertifikaten ist die Aufgabe einer sogenannten „Public-Key Infrastructure" (PKI).

INSIKA®: Kryptografischer Manipulationsschutz für Registrierkassen und Taxameter

Historie

Im Jahresbericht 2003 des BRH wurde auf drohende Steuerausfälle in Milliardenhöhe durch Manipulationsmöglichkeiten in modernen Registrierkassen hingewiesen. In Registrierkassen gespeicherte Daten könnten in vielen Systemen beliebig, ohne die geringsten Spuren zu hinterlassen, verändert werden. Abhilfe sei dringend geboten. Deshalb erarbeitete das BMF in zwei Bund-Länder-Arbeitsgruppen ein Fachkonzept für die Absicherung der in Registrierkassen und Taxametern erzeugten Daten.

Die PTB entwickelte zusammen mit mehreren Partnern aus der Industrie die dafür erforderliche technische Lösung im Rahmen des INSIKA-Projektes. Dieses Vorhaben wurde vom Bundesministerium für Wirtschaft und Technologie als MNPQ-Projekt (Messen, Normen, Prüfen und Qualitätssicherung) gefördert.

Im Juli 2008 sollten die zur Einführung des Systems erforderlichen gesetzlichen Grundlagen im Rahmen des „Aktionsprogramms der Bundesregierung für Recht und Ordnung auf dem Arbeitsmarkt" geschaffen werden. Die entsprechenden Passagen wurden jedoch vor Beginn des Gesetzgebungsverfahrens aus dem Entwurf entfernt.

Das BMF hat am 26.11.2010 ein Schreiben zur „Aufbewahrung digitaler Unterlagen bei Bargeschäften" veröffentlicht. Dieses hebt frühere Erleichterungen für die Aufzeichnungen von Registrierkassen-Daten auf und fordert grundsätzlich die elektronische Aufzeichnung von Einzeltransaktionen. Es wird ferner eine unveränderbare Aufbewahrung gefordert, ohne allerdings konkrete Vorgaben zu machen und die dafür erforderlichen technischen und rechtlichen Rahmenbedingungen zu definieren. Die Forderungen des BRH sind dadurch nicht erfüllt worden.

Das INSIKA-Projekt wurde trotzdem planmäßig weitergeführt. Bereits im Jahr 2008 lagen lauffähige Prototypen der verwendeten Smartcards vor und konnten in Labor- und Praxisversuchen erfolgreich getestet werden. Die Technologie wird momentan in zwei Projekten zur Absicherung von Taxameter-Daten eingesetzt, nachdem das INSIKA-Konzept ab dem Jahr 2010 auf das Taxenumfeld übertragen wurde.

Das INSIKA-Projekt wurde im Februar 2012 erfolgreich abgeschlossen. Das INSIKA-Konzept und insbesondere die daraus entstandenen technischen Verfahren werden nach dem Projektabschluss vom ADM e. V. (Anwendervereinigung Dezentrale Mess-Systeme) unterstützt und weiterentwickelt.

INSIKA wurde so konzipiert, dass nur minimale Auflagen gemacht werden müssen. Die korrekte Nutzung kann über die signierten Belege und signierten Daten überwacht werden, ohne dass dazu Vorgaben für die Bauart der Systeme und eine Zertifizierung der Einhaltung der Vorgaben erforderlich wären. Innovationen im Bereich der Registrierkassen und Taxameter werden daher in keiner Weise behindert.

Da die Kosten für Smartcards vergleichsweise gering sind und der Wettbewerb zwischen den Herstellern von Registrierkassen bzw. Taxametern nicht behindert wird, ist INSIKA mit wesentlich geringeren Kosten verbunden als jedes alternative System.

Kontakt und weiterführende Informationen

Im PTB-Bericht IT-18 „Revisionssicheres System zur Aufzeichnung von Kassenvorgängen und Messinformationen" (abrufbar unter http://dx.doi.org/10.7795/210.20130206a) sind alle wesentlichen Aspekte des INSIKA-Projekts detailliert beschrieben.
Die technischen Spezifikationen sind für Interessierte auf Anfrage frei verfügbar.

Nähere Informationen sind auf **www.insika.de** zu finden.

Kontakt:
INSIKA – ADM e.V.
An der Corvinuskirche 22-26
D – 31515 Wunstorf
eMail: info@insika.de

Das INSIKA-Projekt wurde vom Bundesministerium für Wirtschaft und Technologie unter dem Kennzeichen MNPQ 11/07 gefördert.

Gefördert durch:

Bundesministerium
für Wirtschaft
und Technologie

aufgrund eines Beschlusses
des Deutschen Bundestages