INSIKA®: Kryptografischer Manipulationsschutz für Registrierkassen und Taxameter

Sichere Registrierkassen – internationale Fallbeispiele

Stand: 21. März 2016

INSIKA („INtegrierte SIcherheitslösung für messwertverarbeitende KAssensysteme“) ist ein technologieoffenes Verfahren zur Absicherung digitaler Aufzeichnungen von Bargeschäften mit Hilfe elektronischer Signaturen. Es kann für Registrierkassen, Taxameter, Geldspielgeräte, Wett-Terminals und ähnliche Systeme eingesetzt werden.

In der politischen Diskussion über Sicherungsverfahren werden diese meistens als weitgehend gleichwertig behandelt. In der Realität gibt es allerdings erhebliche Unterschiede beim Sicherheitsniveau und vor allem bei dem zur Implementierung erforderlichen Aufwand. Speziell die abstrakte Forderung nach „Technologieoffenheit“ im Sinn einer reinen Zieldefinition ohne technischen Rahmen, unterstellt, dass praktikable Lösungen auf dieser Basis überhaupt realisierbar sind. Der Beweis dafür wurde noch nicht erbracht.

Diese Analyse stellt typische Beispiele von Sicherungssystemen aus dem europäischen Ausland mit deren Vor- und Nachteilen vor.

Ausgangssituation

Bei vielen Diskussionen über eine „Fiskalisierung“ (also die Einführung besonderer Auflagen für Registrierkassen und ähnliche Geräte mit dem Ziel, sie manipulationssicher zu machen) werden Details weitgehend ausgeblendet.

So wird etwa ganz allgemein von „Zertifizierungen“ als umfassende Lösung für alle nur erdenklichen Probleme gesprochen. Eine Zertifizierung ist jedoch lediglich die Prüfung der Erfüllung bestimmter Anforderungen durch ein System oder Verfahren.[1]

Die Aussagekraft einer Zertifizierung hängt damit

- von der Qualität der Anforderungen,
- ihrer Eignung zur Erfüllung des angestrebten Zwecks sowie
- von der Qualifikation und Neutralität der zertifizierenden Stelle ab.

Der Aufwand für Zertifizierungen wird ebenfalls von diesen Faktoren und zusätzlichen von der Komplexität des zu zertifizierenden Systems bestimmt.

Ohne Beachtung dieser Zusammenhänge ist keine sinnvolle Aussage zum Nutzen einer Zertifizierung möglich.

Es gibt eine Reihe vergleichbarer, ebenso unzulässiger Vereinfachungen, z.B. die mangelnde Unterscheidung verschiedener kryptografischer Verfahren.

Vorgehensweise

Statt einer weiteren, eher theoretischen Analyse[2] werden hier konkrete Praxisbeispiele aus europäischen Ländern vorgestellt, die Gemeinsamkeiten und Unterschiede aufgeführt sowie eine Bewertung vorgenommen.

Es werden ausschließlich technische und praktische Aspekte betrachtet, politische Fragestellungen – wie beispielsweise diejenige nach Art und Ausmaß von Manipulationen – werden hier nicht behandelt.

Kategorisierung verschiedener Lösungsansätze

Zur Unterscheidung der verschiedenen Lösungsansätze wird hier folgende Kategorisierung verwendet:[3]

[1] Hinweis: Kryptografische Zertifikate haben mit dem hier behandelten Thema nichts zu tun. Bei diesen handelt es sich um Datensätze, die einen kryptografischen Schlüssel mit einer Identität (natürliche oder juristische Person) in einer sicheren und vertrauenswürdigen Form verknüpfen.

[2] Hierzu sei auf die bereits existierenden Dokumente verwiesen, z.B.: *Whitepaper: Fiskalsysteme – Anforderungen und Lösungen* (http://www.insika.de/images/stories/INSIKA/Whitepaper_Fiskalsysteme_DE.pdf), Huber, Reckendorf, Zisky: *Die Unveränderbarkeit der (Kassen-) Buchführung nach § 146 Abs. 4 AO im EDV-Zeitalter und INSIKA* in BBK Nr. 12 bis 14, NWB Verlag, 2013

[3] Es handelt es sich um eine etwas vereinfachte Version der Kategorien aus dem Dokument *Sichere Registrierkassen und Technologieoffenheit – eine Analyse*, abrufbar unter: http://www.insika.de/images/stories/INSIKA/analyse_technologieoffenheit_DE.pdf

A: Das Sicherungsverfahren sowie dessen Implementierung sind freigestellt, es gibt lediglich eine Festlegung der zu erreichenden Sicherheitsziele.

B: Das Sicherungsverfahren selbst ist zwar definiert, die Implementierung des Verfahrens, also die konkrete Ausgestaltung der sicherheitsrelevanten Komponenten ist hingegen nicht reglementiert.

C: Sicherungsverfahren und Implementierung sind vorgegeben, für die sicherheitsrelevante Komponente gibt es einen oder mehrere Anbieter.

Fallbeispiele aus dem europäischen Ausland

Die folgenden Beispiele (in alphabetischer Reihenfolge) illustrieren die mögliche Bandbreite von neueren Sicherheitslösungen für Registrierkassen.[4]

Konventionelle Fiskalspeichersysteme[5] werden hier nicht behandelt, da sie aufgrund der technischen Limitierungen für neue Regulierungen praktisch nicht in Frage kommen.

Belgien (Kategorie C)

In Belgien wurde im Dezember 2009 eine Fiskalkassenpflicht nur für die Gastronomie beschlossen – politisch stand diese Maßnahme in unmittelbarem Zusammenhang mit der Herabsetzung des Umsatzsteuersatzes für diese Branche. Der Einführungstermin wurde aufgrund von Schwierigkeiten bei Konzeption und Umsetzung mehrfach verschoben, so dass ein einigermaßen flächendeckender Betrieb erst 2016 erreicht wurde.

Technik

Jede Registrierkasse ist an eine vorgegebene Schnittstelle – eine „Blackbox" (mehrere Hersteller am Markt, Marktpreis für Anwender ca. € 300 bis 400) – anzuschließen, in die eine von der Finanzverwaltung kostenlos ausgegebene Smartcard eingelegt wird. Diese signiert die Verkaufsdaten; die Blackbox speichert parallel zur Kasse einen Teil der Transaktionsdaten. Auf diese Daten können Prüfer über eine SD-Card zugreifen.

Darüber hinaus gibt es viele, komplexe Anforderungen an die Kassensoftware. Neben Smartcard und Blackbox müssen daher auch die Programme der Registrierkasse zertifiziert werden. Diese Zertifizierung erfolgt durch das Finanzministerium.

Zusätzlich gibt es einen aufwändigen Online-Registrierungsprozess für sämtliche Marktteilnehmer (Hersteller, Händler, Anwender) sowie jede einzelne Smartcard, Blackbox und Kasse.

Zeitplan

Termin	Ereignis
12/2009	Gesetz
06/2013	Technische Richtlinie
10/2013	Änderung Richtlinie
01/2015	Beginn Kassenpflicht
in 2016	Flächendeckender Einsatz

Bewertung

Politische Vorgaben und mangelndes Know-How in den Behörden führten zu einer extremen Komplexität, die viele Verzögerungen sowie hohe Einmal- und laufenden Kosten verursacht hat.

Frankreich (Kategorie A)

Ende 2015 wurde ein Gesetz verabschiedet, das den Einsatz nicht-zertifizierter Registrierkassen ab dem 01.01.2018 verbietet.

Technik

Das Gesetz macht keinerlei technische Vorgaben. Es gibt ein Unternehmen, das eine Zertifizierung anhand einer speziell dafür erstellen Norm „NF525" anbietet. Diese versucht der Anbieter momentan als de-facto-Standard zu etablieren. Die Eignung der „NF525" zur Vermeidung von Manipulationen ist fraglich, da wesentliche Sicherheitselemente fehlen, so etwa der verpflichtende Beleg als Nachweis einer korrekten Erfassung; die Erfüllung des in nahezu allen Staaten geforderten Tatbestandmerkmals „Vollständigkeit der Daten" ist damit weder prüf- noch nachweisbar.

Zeitplan

Termin	Ereignis
12/2013	Strafverschärfung für Manipulationen
06/2014	Vorstellung der NF525
12/2015	Gesetz über zertifizierte Kassen
01/2018	Inkrafttreten des Gesetzes aus 12/2015

Bewertung

Bisher herrscht Unklarheit, wie die gesetzlichen Anforderungen erfüllt werden können. Dies hat eine massive Verunsicherung bei den meisten von der Regelung Betroffenen ausgelöst.

[4] Die wenigsten Verfahren lassen sich direkt auf Taxameter, Geldspielgeräte usw. übertragen, so dass diese Anwendungsfälle hier nicht behandelt werden.

[5] Typische Eigenschaften: mechanisch geschützter Speicher, keine Einzelaufzeichnung, Gerätezertifizierung, Prüfung erfordert direkten Zugriff auf das Gerät.

Kroatien (Kategorie C)

Seit dem 01.01.2013 müssen Registrierkassen in Kroatien online mit einem Rechenzentrum, das im Auftrag des Finanzministeriums arbeitet, verbunden sein. Das System wurde praktisch ohne Übergangsfrist eingeführt.

Technik

Registrierkassen werden über eine Internet-Verbindung und eine recht aufwändige SOAP-Schnittstelle an ein Rechenzentrum angeschlossen. Jeder Beleg wird in Echtzeit übertragen, zentral gespeichert und eine auf dem Beleg abzudruckende Signatur an die Kasse zurückgeliefert.

Eine Zertifizierung der Kassen ist bei diesem Verfahren nicht erforderlich.

Zeitplan

Termin	Ereignis
10/2012	Veröffentlichung Spezifikation
11/2012	Gesetz verabschiedet
1/2013	Start Echtbetrieb
7/2013	Ende der Übergangsfrist, Strafen bei Nichtnutzung

Bewertung

Die technische Lösung ist kritisch zu sehen: Die Abhängigkeit von Internet-Verbindungen und die technischen Anforderungen verursachen hohe Kosten und schließen viele Systeme vom kroatischen Markt aus.[6]

Auffallend ist jedoch, dass auf der Basis eines fertig entwickelten Systems eine äußerst zügige Einführung möglich war.

Niederlande (Kategorie A)

Auf Initiative der Finanzverwaltung wurde die „Stichting Betrouwbare Afrekensystemen“ (Stiftung Vertrauenswürdige Kassensysteme) gegründet. Diese bietet Mitgliedern eine Zertifizierung von Registrierkassen an. Nutzern wird unverbindlich in Aussicht gestellt, dass Betriebsprüfungen bei ihnen vereinfacht ablaufen.

Technik

Es erfolgt eine Zertifizierung durch von der Stiftung beauftragte Wirtschaftsprüfer auf Basis eines aufwändigen Kriterienkatalogs. Durch die Abfrage vieler Detailaspekte während der Zertifizierung wird versucht, Manipulationsmöglichkeiten zu verhindern. Konkrete, technische Vorgaben existieren nicht, stattdessen wird stark auf Compliance, also Vertrauen in die Hersteller gesetzt.

Zeitplan

Termin	Ereignis
04/2011	Gründung der Stiftung
01/2013	Erste Zertifizierungen

Bewertung

Die Zertifizierung ist aufgrund fehlender Rechtssicherheit praktisch sinnlos. Dementsprechend ist die Nachfrage im Markt sehr gering.

Österreich (Kategorie C)

In Österreich besteht eine Kassenpflicht seit dem 01.01.2016. Am 01.01.2017 müssen alle Kassen mit einer technischen Sicherheitseinrichtung gemäß Registrierkassensicherheitsverordnung (RKSV) ausgestattet sein.

Technik

Die Sicherheitseinrichtung basiert auf digitalen Signaturen von Buchungsdaten. Die Signaturen müssen als QR-Code auf die Belege gedruckt und mit den Buchungsdaten gespeichert werden. Aufgrund der Struktur des Verfahrens ist keine Zertifizierung der Registrierkassen erforderlich.

Die Lösung ist in vielen Aspekten dem INSIKA-Verfahren ähnlich; allerdings finden statt spezieller Smartcards Standard-Signaturkarten Verwendung, was sich als nachteilig herausgestellt hat.[7]

Zeitplan

Termin	Ereignis
12/2012	Beginn politische Debatte
07/2015	Gesetz verabschiedet
09/2015	Entwurf RKSV
12/2015	RKSV rechtskräftig
01/2016	Stichtag Kassenpflicht
01/2017	Stichtag für Einsatz der Sicherheitseinrichtung laut RKSV

Bewertung

Das Verfahren wurde ohne Erprobung in der Praxis spezifiziert und in die Verordnung übernommen. Auch wenn die Anlehnung an INSIKA grundsätzliche Architekturprobleme verhindert hat, bedingen viele Details eine unnötig aufwändige Umsetzung. Diese wurde weitergehend dadurch erschwert, dass viele Detailklärungen erst im laufenden Einführungsprozess erfolgten.

[6] Typische preiswerte Kassensysteme können nicht oder nur mit unverhältnismäßigem Aufwand um die nötigen Kommunikationsprotokolle sowie die Internet-Anbindung erweitert werden.

[7] Siehe *Analyse der österreichischen Registrierkassensicherheitsverordnung vom 1. September 2015*, abrufbar unter http://www.insika.de/images/stories/INSIKA/Analyse_RKSV_oesterreich.pdf

Die Auslagerung elementarer Sicherheitsfunktionalitäten (Summenspeicher und Sequenzzähler) von der Smartcard in die Kasse hat überdies zu Sicherheitslücken geführt.

Portugal (Kategorie B)

Registrierkassen müssen ein Sicherungsverfahren auf Basis digitaler Signaturen beinhalten. Die Registrierkassen werden vom Finanzministerium zertifiziert.

Technik

Kern des Verfahrens ist die Vorschrift, Daten im von der OECD standardisierten SAF-T-Format mit zusätzlichen Erweiterungen zu liefern. Die Absicherung der Daten erfolgt über eine Signatur, die per Software ohne eine Hardware-Sicherheitskomponente erzeugt wird.

Zeitplan

Termin	Ereignis
06/2010	Verordnung
01/2011	Kassenpflicht für Unternehmen über € 250.000 Umsatz
01/2012	Kassenpflicht für Unternehmen über € 150.000 Umsatz
01/2012	Nachbesserung der Verordnung
11/2013	Nachbesserung der Verordnung
07/2014	Nachbesserung der Verordnung

Bewertung

Das Verfahren ist konzeptionell stark mangelhaft, was zu massiven Sicherheitslücken und zu laufenden Nachbesserungen geführt hat. Diese Nachbesserungen haben die Grundprobleme jedoch immer noch nicht beseitigt.

Schweden (Kategorie C)

Das schwedische Verfahren war Vorbild für die belgische Lösung. Hier wird allerdings statt einer Zertifizierung der Registrierkassen auf eine Konformitätserklärung der Hersteller gesetzt. Für Großunternehmen kann die Finanzverwaltung Ausnahmen von Fiskalkassenpflicht genehmigen – transparente Kriterien existieren jedoch nicht dafür.

Technik

Jede Registrierkasse muss über eine vorgegebene Schnittstelle mit einer zertifizierten Fiskalbox verbunden sein. Diese Box erzeugt eine Art Signatur und speichert einen Teil der Verkaufsdaten parallel zur Kasse. An die Funktionen der Kassen wird eine Reihe von Anforderungen gestellt, die diverse Funktionseinschränkungen nach sich ziehen.

Zeitplan

Termin	Ereignis
06/2006	Beginn der politischen Diskussion
03/2007	Gesetzentwurf vorgelegt
06/2008	Gesetz verabschiedet
01/2009	Technische Richtlinie
01/2010	Kassenpflicht

Bewertung

Neben dem hohen Aufwand ist die Konformitätserklärung des Herstellers ein Problem. Dadurch besteht für Hersteller und Anwender keine Rechtssicherheit. Trotz zertifizierter Fiskalbox und Herstellererklärung können Prüfer die Daten verwerfen.

Analyse

Auffällig ist, dass fast alle hier vorgestellten Lösungen außerordentlich komplex sind. In mehreren Systemen gibt es – mittlerweile bekannt gewordene – Sicherheitslücken. Ein größerer Teil der Lösungen ist zwar grundsätzlich tauglich, der dafür erforderliche Aufwand erscheint aber deutlich zu hoch.

In den meisten hier vorgestellten Fällen wurde zuerst die gesetzliche Regelung geschaffen, um die konkrete Ausgestaltung erst danach zu beginnen. Das hat stets zu Verzögerungen, zum Teil von erheblichem Ausmaß, geführt. So wurde das entsprechende Gesetz in Belgien im Dezember 2009 erlassen; der ursprüngliche Einführungstermin sollte der 01.01.2013 sein. Die Verordnung mit den technischen Details war jedoch erst Mitte 2013 verfügbar, so dass die Umstellung selbst zum mehrfach verschobenen Einführungstermin 01.01.2016 noch nicht vollständig abgeschlossen war.

Für Kontrollen und Prüfungen existierte in den meisten Fällen vor der Einführung gar kein oder kein ausgereiftes Konzept. Das hat entweder zu Fehlkonzeptionen (z.B. zum Verzicht auf kontrollfähige Belege) oder zumindest zu unnötigem Aufwand geführt.

Von den hier diskutierten praktischen Lösungen verfolgen zwei den Grundgedanken, keinerlei technische Vorgaben zu machen und die Lösungsfindung vollständig dem Markt zu überlassen (Niederlande und Frankreich). Den niederländischen Ansatz muss man als gescheitert betrachten. In Frankreich sind momentan vor allem eine große Verunsicherung im Markt und der Versuch eines Anbieters, ein teures und aufwändiges Zertifizierungsmonopol zu etablieren, zu beobachten.

Fazit

Um schnell und effektiv zu einer sicheren und kostengünstigen Lösung zu kommen, sind die folgenden Faktoren entscheidend:

- Lediglich allgemeine (Ziel-)Vorgaben sind nicht ausreichend, ein funktionierendes Sicherungsverfahren einzuführen.
- Die fachlichen Anforderungen und entscheidende technische Eckdaten müssen klar und unmissverständlich definiert sein.
- Es muss ein fertig entwickeltes, vollständig dokumentiertes, offenes, patentfreies und vor allem im Feld erprobtes Verfahren eingeführt werden, statt Spezifikation, Entwicklung und Erprobung unter hohem Zeit- und politischem Erfolgsdruck durchführen zu müssen.
- Ein Verfahren muss so einfach wie möglich sein. Komplexität erhöht nicht nur Kosten und Risiken, sondern setzt regelmäßig die Prüfbarkeit als solche, zumindest eine Prüfung in angemessener Zeit deutlich herab. Allein die Frage, ob das System noch dem zum Zeitpunkt der Zulassung bzw. Zertifizierung entspricht, ist bei einigen hier vorgestellten Systemen nur mit größtem Aufwand zu beantworten. Eine eingeschränkte oder mangelnde Prüfbarkeit mindert zugleich die Rechtssicherheit auf Seiten des Kassenanwenders.

Bei der Entwicklung des INSIKA-Verfahrens wurden diese Zielvorgaben berücksichtigt. Dementsprechend sind sie bei der Umsetzung beachtet und erfüllt worden.

INSIKA und ADM e.V.

INSIKA wurde in den Jahren 2008 bis 2012 auf Grundlage eines Konzepts der deutschen Finanzbehörden von der Physikalisch-Technischen Bundesanstalt in einem Gemeinschaftsprojekt mit der Industrie konzipiert, entwickelt und erprobt. Seit dem erfolgreichen Projektabschluss werden das Konzept und die daraus entstandenen technischen Verfahren vom ADM e.V. (Anwendervereinigung Dezentrale Mess-Systeme) unterstützt und weiterentwickelt.

Das INISKA-Verfahren kann ohne Patente, Lizenzkosten oder Ähnliches genutzt werden. Es bestehen daher keine wirtschaftlichen Interessen des ADM e.V. Das Hauptanliegen der Mitglieder liegt vielmehr darin, ein möglichst sicheres, preiswertes und einfach zu nutzendes Verfahren zur Absicherung elektronischer Aufzeichnungen von Bargeschäften zu etablieren – und dabei vor allem eine echte Alternative zu den aufwändigen Zertifizierungsverfahren konventioneller „Fiskalkassensysteme“ zu bieten. Ein besonderer Schwerpunkt ist Rechtssicherheit für die Anwender.

Kontakt

INSIKA – ADM e.V.
An der Corvinuskirche 22-26
D-31515 Wunstorf

www.insika.de

E-Mail: info@insika.de

Übersicht	B	F	HR	NL	A	P	S	INSIKA
Kategorie	C	A	C	A	C	B	C	C
Kassenpflicht	Ja	Nein	Ja	Nein	Ja	Ja	Ja	Sinnvoll
Belegpflicht	Ja	Nein	Ja	Nein	Ja	Ja	Ja	Ja
Gesamtsystemzertifizierung *	Ja	Ja	Nein	Ja	Nein	Ja	Ja **	Nein
Vorgaben für Sicherungsverfahren	Ja	Teilw.	Ja	Nein	Ja	Ja	Ja	Ja
Vorgaben für Kassensoftware ***	Ja	Ja	Nein	Ja	Nein	Ja	Ja	Nein
Vorgaben für zu liefernde Datenformate ****	Teilw.	Nein	Ja	Nein	Teilw.	Ja	Teilw.	Ja
Sicherheitsniveau (gering: -, mittel: o, hoch: +)	+	-	+	-	+	o	+	+
Prüfbarkeit (schlecht: -, mittel: o, gut: +)	o	-	+	-	o	+	o	+
Rechtssicherheit für Anwender	Ja	?	Ja	Nein	Ja	Ja	Teilw.	Ja

* Zertifizierung des Gesamtsystems und nicht nur der Sicherheitseinrichtung
** Herstellererklärung für Kassensoftware, Zertifizierung für Fiskalbox
*** Gemeint sind Vorgaben, die darüber hinaus gehen, die Sicherheitseinrichtung nutzen zu müssen
**** „Teilw.“ bedeutet hier, dass nur ein Teil der prüfungsrelevanten Daten standardisiert ist – der andere Teil ist herstellerspezifisch