

14 Irrtümer über INSIKA

Stand: 17. März 2016 (aktualisiert)

Die Debatte über sichere Registrierkassen, Taxameter und ähnliche Geräte wird verstärkt in der Öffentlichkeit und der Politik statt unter Sicherheits- und Branchenexperten geführt. In Laufe dieses Prozesses hat sich eine Reihe von Irrtümern in die Diskussion eingeschlichen.

Die häufigsten dieser Fehlinformationen sollen hier anhand der Fakten aufgeklärt werden.

1. Irrtum „INSIKA ist unsicher“

Im Wesentlichen handelt es sich dabei um folgende Aussagen:

1. *INSIKA kann die Nicht-Eingabe oder die Verwendung von „Zweit-Kassen“ nicht verhindern.*
2. *Eine Manipulationssoftware kann das Signieren von Geschäftsvorfällen unterdrücken.*
3. *Auf Belegen können QR-Codes gedruckt werden, die auf einen falschen Verifikationsserver verweisen.*
4. *Das Verfahren ist generell unsicher.*

Fakten

Wie jedes andere denkbare Verfahren für sichere Registrierkassen kann die Technik alleine nicht für Sicherheit sorgen. Es sind immer flankierende organisatorische und rechtliche Maßnahmen erforderlich.

Gerade für die ersten beiden hier genannten Fälle bietet das INSIKA-Verfahren einen wirkungsvollen und effizienten Kontrollmechanismus in Form der Belegsignatur. Voraussetzung dafür sind lediglich klare gesetzliche Regelungen zu einer Belegausgabepflicht sowie entsprechende Kontrollen. Mit jedem nicht ausgegebenen und jedem nicht korrekt signierten Beleg steigt das Entdeckungsrisiko. Die Belegprüfung kann zu jeder Zeit nach dem Abschluss des Geschäftsvorfalles erfolgen.

Punkt 3 erfordert, wie bei jedem Internet-Link, eine kurze Augenscheinkontrolle der korrekten Web-Adresse.

Zu Punkt 4 ist festzustellen, dass kein erfolgreicher Angriff auf die Sicherheitsmechanismen INSIKA bekannt ist. Die Spezifikation sowie Test-Smartcards sind seit 2009 öffentlich verfügbar, so dass bereits sehr viel Zeit für Analysen oder Angriffsversuche zur Verfügung stand.

Die wesentlichen Sicherheitsaspekte des INSIKA-Verfahrens werden im Dokument *Wie werden Registrierkassen und Taxameter sicher?* erläutert.

2. Irrtum „Probleme mit INSIKA“

Mit INSIKA gibt es Probleme.

Eine nähere Beschreibung der Probleme fehlt jedoch.

Fakten

Bei den seit 2010 im Einsatz befindlichen INSIKA-Systemen wurden keine konzeptbedingten Probleme festgestellt. Bei keiner der an Entwicklung, Test und Weiterbetreuung beteiligten Institutionen und Personen ist ein konkreter Bericht über Probleme eingegangen.

3. Irrtum „Technisch überholt“

INSIKA ist technisch überholt.

Diese Aussage wird nicht mit Details oder Fakten unterlegt. Grundsätzlich kann sich ein technisches Verfahren nur auf zwei verschiedene Arten überholen:

1. Die verwendeten Komponenten entsprechen nicht mehr dem Stand der Technik oder
2. es gibt inzwischen neuere und zugleich den (funktionalen und nichtfunktionalen) Anforderungen besser genügende Verfahren.

Fakten

Zu 1.: INSIKA verwendet hochsichere Standard-Kryptografieverfahren und -komponenten, die bereits in einer Vielzahl anderer technischer Anwendungen eingesetzt werden. Wenn diese bei INSIKA eingesetzten Verfahren (also kryptografische Algorithmen) oder die verwendeten Komponenten (Signaturerstellungseinheiten) nicht mehr dem Stand der Technik entsprechen sollten, könnten sie jederzeit durch neuere Varianten ersetzt werden, ohne das INSIKA-Verfahren selbst ändern zu müssen. So ist etwa ein Wechsel von ECDSA-192 auf ECDSA-256 konkret geplant. Das gleiche gilt für Anpassungen im Bereich der abzusichernden Daten, die durch Änderungen der jeweiligen sog. Profile leicht möglich sind.

Zu 2.: Es sind zwar einige neuere Verfahren bekannt (z.B. aus Belgien oder Österreich). Diese

sind jedoch weder einfacher oder sicherer noch preiswerter – und damit in keinem Fall „besser“.

4. Irrtum „Technologieoffenheit und Innovationsfeindlichkeit“

INSIKA ist nicht technologieoffen und damit innovationsfeindlich.

Technologieoffenheit muss hier zum einen dazu dienen, Weiter- und Neuentwicklungen bei den Registrierkassen selbst nicht zu behindern und damit die Innovationsfähigkeit der Anbieter zu schützen. Zum anderen muss sie bei Bedarf die Anpassung an neue Risiken und höhere Sicherheitsstandards erlauben.

Fakten

INSIKA ist mit dem Ziel entwickelt worden, die Eingriffe in die abzusichernden Systeme zu minimieren, um deren Weiterentwicklung nicht zu behindern. Dieses Ziel wurde sowohl aus Sicht der INSIKA-Projektgruppe als auch nach Meinung der Hersteller, die INSIKA integriert haben, voll erreicht. Sehr wichtig dabei ist, dass die abgesicherten Systeme nicht zertifiziert werden müssen.

INSIKA definiert nach dem Vorbild des Signaturgesetzes lediglich ein Verfahren und lässt bei der Implementierung große Freiheiten. Nur die eingesetzte Signaturerstellungseinheit muss zertifiziert und behördlich anerkannt sein, um die erforderliche Rechtssicherheit herstellen zu können.

Eine ausführliche Analyse findet sich im INSIKA-Dokument *Sichere Registrierkassen und Technologieoffenheit – eine Analyse*.

5. Irrtum „Sichere Lösungen auf Basis allgemeiner Anforderungen sind möglich“

Die Ausgestaltung der Technik sicherer Registrierkassen soll „(technologie-) offen“ sein. Der Gesetzgeber soll deshalb nur allgemeine Anforderungen formulieren.

Diese Forderung setzt stillschweigend voraus, dass Technologieoffenheit das Fehlen konkreter Regeln bedeutet. Genauere Vorstellungen dazu bestehen offenbar nicht. Beispiele sicherer Systeme auf Basis nur allgemeiner Anforderungen werden nicht genannt.

Fakten

„Technologieoffen“ bedeutet nicht, dass nur unspezifische Anforderungen gestellt werden, son-

dern dass die genaue Umsetzung von durchaus konkreten Anforderungen nicht vorgegeben wird.

Es ist bisher weltweit keine einzige Lösung bekannt, die allein auf allgemeinen Anforderungen basiert und gleichzeitig als sicher anerkannt ist. Alle existierenden sicheren Verfahren basieren auf strengen und detaillierten Vorgaben. Die meisten dieser Verfahren greifen sehr tief in die zu schützenden Systeme ein. INSIKA ist demgegenüber so konzipiert, dass diese Eingriffe auf ein absolutes Minimum reduziert werden.

Alle Verfahren, die lediglich auf unspezifischen Vorgaben basieren (i.d.R. Softwarezertifizierungen), haben keinerlei Beweiskraft zugunsten der Anwender und gelten damit als unsicher.

6. Irrtum „Hohe Einmalkosten“

INSIKA verursacht hohe Einmalkosten von Hunderten Millionen oder sogar Milliarden Euro.

Für die Initialkosten beim Einsatz von INSIKA werden je nach Urheber sehr unterschiedliche Werte genannt. Die werden dann meistens mit einer geschätzten Anzahl von Registrierkassen in Deutschland multipliziert.

Fakten

Für die Umstellung von Bestandsgeräten fallen unweigerlich Kosten an. Durch den gewählten technischen, „minimalinvasiven“ Ansatz sind diese Kosten geringer als bei jedem anderen bekannten Sicherungssystem. Die teilweise genannten € 1.200 Subvention im Taxi-Bereich haben aufgrund der völlig anderen Voraussetzungen (Einbau in Fahrzeug, geeichte Taxameter) nichts mit den Kosten bei Registrierkassen zu tun.

Die Einfachheit des INSIKA-Verfahrens sowie der Wettbewerb unter den Anbietern werden dafür sorgen, dass Neugeräte sich nicht oder nur minimal verteuern.

Auf der anderen Seite sind Kosteneinsparungen durch erheblich verringerten Aufwand für Dokumentation und Betriebsprüfungen zu erwarten.

7. Irrtum „Laufende Kosten“

INSIKA verursacht laufende Kosten durch Softwarewartung, Support und Schulungen.

Fakten

Nach der einmaligen Einführung erfordert INSIKA keine Softwareanpassungen, sofern Spezifikation und Schnittstelle stabil bleiben. Es gibt

jedoch keinen bekannten Grund, warum es solche Änderungen geben sollte. Die Spezifikation ist bereits seit dem Jahr 2009 stabil.

Ohne Softwareänderungen entstehen auch keine der genannten Kosten. Besondere Schulungen für das Kassenpersonal sind nicht erforderlich, da sich die Bedienabläufe nicht verändern.

Lediglich ein möglicher Austausch einer Smartcard während der normalen Nutzungsdauer einer Registrierkasse würde Folgekosten verursachen.

8. Irrtum „Bürokratiekosten“

Sichere Registrierkassen verursachen Bürokratie und damit Bürokratiekosten.

Fakten

Es entstehen Anschaffungs- und Umrüstkosten. Bürokratiekosten werden demgegenüber allerdings deutlich verringert, da Betriebsprüfungen in bargeldintensiven Unternehmen ganz erheblich vereinfacht werden.

9. Irrtum „Abhängigkeit“

Die Nutzung von INSIKA führt zur Abhängigkeit von nur einem Anbieter.

Fakten

Bei INSIKA handelt es sich um ein Verfahren, und nicht um ein Produkt. Das Verfahren ist veröffentlicht und frei von Patenten oder sonstigen Schutzrechten. Lediglich der Name „INSIKA“ ist zur Verhinderung einer missbräuchlichen Verwendung als Warenzeichen eingetragen.

Die Sicherheitskomponenten (Signaturerstellungseinheiten, Verifikationssoftware usw.) können bei Bedarf von verschiedenen Anbietern implementiert werden (Voraussetzung für die praktische Nutzbarkeit ist natürlich immer eine behördliche Anerkennung der jeweiligen Implementierung).

10. Irrtum „Europarechtliche Probleme“

Eine gesetzliche Einführung von INSIKA verstößt gegen Europarecht.

INSIKA entspricht nicht den europäischen Sicherheitsanforderungen.

Fakten

Die gesetzliche Einführung einer Verpflichtung zur Nutzung einer Signaturerstellungseinheit nach

dem INSIKA-Konzept beim Einsatz in Registrierkassen und kassenähnlichen Systemen verstößt weder gegen

- die Warenverkehrsfreiheit nach Artikeln 28 bis 37 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV), da Gründe des öffentlichen Interesses vorliegen, namentlich die Erhebung von Steuern und Abgaben

noch gegen

- die Richtlinie 2004/22/EG des Europäischen Parlaments und des Rates vom 31. März 2004 über Messgeräte (Measuring Instruments Directive – MID)

oder

- die Richtlinie 2014/31/EG des Europäischen Parlaments und des vom 26. Februar 2014 zur Angleichung der Rechtsvorschriften der Mitgliedstaaten betreffend die Bereitstellung nichtselbsttätiger Waagen auf dem Markt (NAWID),

da die Funktionen der sicheren Signaturerstellungseinheit nach dem INSIKA-Konzept bei Taxametern und Waagen sowohl auf den europarechtlich relevanten Sicherheitsanforderungen aufbauen, als auch diesen gegenüber präzise abgegrenzt sind.

Für Registrierkassen selbst existieren keinerlei europäische Sicherheitsanforderungen.

Allenfalls könnte eine Notifizierung der entsprechenden gesetzlichen Regelungen gemäß der Richtlinie 98/34/EG des Europäischen Parlaments und des Rates vom 22. Juni 1998 über ein „Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften“ in Betracht kommen. Bisherige Fiskalsysteme – soweit überhaupt notifiziert – wurden durch die Notifizierung weder aufgehoben noch wesentlich verändert.

11. Irrtum „Rufschädigung möglich“

Belege mit verifizierbaren Signaturen können beim Fehlschlag einer Verifikation durch Endkunden zum Verdacht der Steuerhinterziehung führen.

Fakten

Es gibt keinen Grund zur Annahme, dass eine korrekte und getestete INSIKA-Implementierung Belege erzeugt, die nicht positiv verifiziert werden können.

Selbst wenn das Ergebnis einer Verifikation negativ sein sollte, wird der Hinweis darauf durch Endkunden oder Mitarbeiter der Finanzverwaltung eine wertvolle Information für den Unternehmer sein, weil damit ein wesentlich größeres Problem bei einer kommenden Betriebsprüfung verhindert werden könnte.

12. Irrtum „Freiwilliger Einsatz“

Ein freiwilliger Einsatz von Sicherheitseinrichtungen (ob INSIKA oder andere Verfahren) kann Probleme mit Manipulationen ebenfalls lösen.

Fakten

Sicherheit und eine entsprechende Beweiskraft für Steuerpflichtige sind beim freiwilligen Einsatz höchstens für die Forderung nach „Unveränderbarkeit“ erzielbar.

Die Anforderungen der Abgabenordnung, dass die Aufzeichnungen vollständig, richtig, zeitgerecht und geordnet sein müssen, sind jedoch ausschließlich mit einem verpflichtenden Einsatz und entsprechenden Kontrollen zu erreichen.

Eine nähere Darstellung findet sich im Dokument *Wie werden Registrierkassen und Taxameter sicher?*

13. Irrtum „Software-Zertifizierung“

Eine Softwarezertifizierung ist eine einfachere und preiswertere Alternative zu Sicherheitslösungen mit klaren Vorgaben und einer sicheren Hardwarekomponente.

Fakten

Sicherheitslösungen allein auf Softwarebasis vermögen keine Manipulationssicherheit zu gewährleisten. Ohne spezielle hardwarebasierte Sicherheitskomponenten ist jedes System grundsätzlich angreifbar – speziell diejenigen auf offenen Plattformen wie Windows, Linux usw.

Manipulationssicherheit nach dem Stand der Technik ist heute allein durch eine kombinierte Hardware/Software-Lösung zu erzielen.

Darüber hinaus sind Softwarezertifizierungen höchst aufwändig, da statt einer kleinen Sicherheitskomponente ein komplexes Gesamtsystem geprüft werden muss. Jede Veränderung an der Software erfordert zudem eine Erneuerung der Zertifizierung, was dieses Konzept besonders innovationsfeindlich und kostenaufwändig macht.

14. Irrtum „Aktuelle Rechtslage ausreichend“

Es reicht aus, die aktuelle Rechtslage einfach nur konsequent zu vollziehen.

Fakten

Das Problem von Kassenmanipulationen konnte in den letzten zwei Jahrzehnten nicht gelöst werden. Stattdessen werden Manipulationen immer komplexer und sind daher ohne Spezialausbildung im IT-Bereich nicht mehr zu entdecken.

Das führt immer mehr dazu, dass sich Anwender von Registrierkassen, insbesondere bei Betriebsprüfungen, pauschal verdächtig sehen. Mangels technischer und rechtlicher Grundlagen sind sie dann nicht in der Lage, die Ordnungsmäßigkeit ihrer Aufzeichnung nachzuweisen.

INSIKA und ADM e.V.

INSIKA („INtegrierte SIcherheitslösung für messwertverarbeitende KAssensysteme“) wurde auf der Grundlage eines Konzepts der deutschen Finanzbehörden von der Physikalisch-Technischen Bundesanstalt von 2008 bis 2012 in einem Gemeinschaftsprojekt mit der Industrie konzipiert, entwickelt und erprobt. Seit erfolgreichem 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 konventionellen „Fiskalkassensystemen“ zu bieten. Ein besonderer Schwerpunkt ist die Rechtssicherheit für die Anwender der Systeme.

Kontakt

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