INSIKA®: Kryptografischer Manipulationsschutz für Registrierkassen und Taxameter

Analyse des Entwurfs der österreichischen Registrierkassensicherheits-Verordnung vom 30. Juni 2015

Stand: 8. Juli 2015

Zusammenfassung

Das österreichische Steuerreformgesetz 2015/2016 beinhaltet eine Registrierkassen- und Belegpflicht sowie die Verpflichtung zum Einsatz einer technischen Manipulationssicherung. Diese wird im Entwurf der Registrierkassensicherheits-Verordnung vom 30. Juni 2015 genauer beschrieben.

Das gewählte Verfahren nutzt Grundideen des INSIKA-Konzepts, basiert also auf elektronischen Signaturen, die durch eine Signaturerstellungseinheit (Smartcard) erstellt werden. Es weicht aber in wesentlichen Punkten davon ab. Die Abweichungen bedingen höheren Aufwand, höhere Kosten und eine verringerte Sicherheit. Die meisten Nachteile treffen die Anwender. Zwei Sicherheitslücken, davon eine erhebliche, sind in dieser Analyse dargestellt. Die Beweiskraft eines Sicherheitssystems mit bekannten Schwächen ist fraglich.

Für Großunternehmen sieht die Verordnung eine Ausnahmeregelung vor, die ein Arbeiten ohne Signaturerstellungseinheiten erlauben soll. Die Auflagen sind allerdings so streng, dass diese Ausnahmeregelung in der Praxis kaum nutzbar ist.

INSIKA und ADM e.V.

Das INSIKA-Verfahren („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 entwickelt und erprobt. Nach erfolgreichem Projektabschluss werden das INSIKA-Konzept und insbesondere 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 (wie sie vor allem bei Registrierkassen und ähnlichen Geräten vorkommen) zu etablieren – und dabei vor allem eine echte Alternative zu konventionellen, sehr aufwändigen „Fiskalkassensystemen“ zu bieten.

Weitere Informationen sind auf www.insika.de frei abrufbar. Lediglich der Abruf der technischen Spezifikationen erfordert eine einfache und kostenlose Registrierung.

Registrierkassensicherheits-Verordnung

Im österreichischen Steuerreformgesetz 2015/2016, das am 7. Juli 2015 im Nationalrat beschlossen wurde, sind eine Registrierkassenpflicht sowie ein kryptografischer Manipulationsschutz für Registrierkassen verankert. Die weiteren Details sollen durch die „Registrierkassensicherheits-Verordnung“ („RKS-V“) bestimmt werden. Der in diesem Dokument analysierte Entwurf der Verordnung wurde am 30. Juni 2015 veröffentlicht.

Eine Anforderungsspezifikation für das in der RKS-V beschriebene Verfahren (im Folgenden „RKS-V-Verfahren“) ist dem ADM e.V. ebenso wenig bekannt wie eine technische Detailspezifikation. Daher konnte die Analyse nur auf Basis des Verordnungstextes, also auf der konzeptionellen Ebene in Gegenüberstellung zum INSIKA-Verfahren erfolgen.

Die genaue Entstehungsgeschichte der RKS-V ist nicht bekannt. Die Vermutung liegt nahe, dass es Ziel der RKS-V ist, ein ähnliches System wie INSIKA zu spezifizieren, dabei jedoch mit Standard-Signaturkarten arbeiten zu können.

Analyse der technischen Unterschiede zu INSIKA

INSIKA verwendet als Signaturerstellungseinheiten gegenwärtig Smartcards (auch HSMs wären prinzipiell einsetzbar). Anstelle von „Signaturerstellungseinheiten“ wird deshalb im Folgenden vereinfachend der Begriff „Smartcards“ benutzt.

Die INSIKA-Smartcards sind „sichere Signaturerstellungseinheiten mit erweiterter Funktionalität“. Die Zusatzfunktionen sind exakt auf die An-

forderungen abgestimmt. Alle wesentlichen Sicherheitsfunktionen laufen kartenintern ab, also ohne die Möglichkeit einer Beeinflussung von außen. Der Verzicht auf spezielle Smartcards beim RKS-V-Verfahren führt zu erheblichen Unterschieden gegenüber einer Lösung nach dem INSIKA-Konzept. Die Auswirkungen sollen hier näher analysiert werden.

Fehlende Sequenzzähler in der Smartcard

Beschreibung

Die von der Smartcard verwalteten und automatisch in den Signaturvorgang einbezogenen Sequenzzähler sind bei INSIKA der zentrale Mechanismus zur Sicherstellung der Vollständigkeit der Daten. Ohne diesen nicht-beeinflussbaren Zähler wird ein anderes System zur Erkennung fehlender Aufzeichnungen benötigt.

Ersatzmechanismus

Der Sequenzzähler wird von der Registrierkasse verwaltet. Es erfolgt eine Verkettung der Buchungen durch die Aufnahme eines Teils der Signatur der vorherigen Buchung. Bei der ersten Buchung ist hier ein von der Finanzverwaltung bereitgestellter Initialwert zu verwenden.

Bewertung

Auf den ersten Blick erfüllt das Verfahren den Zweck. Es bleiben jedoch Sicherheitslücken (siehe unten). Die Verwaltung des Initialwertes ist für den Anwender komplex und vor allem fehleranfällig. Bei Geräten wie Taxametern ist die Eingabe solcher Daten aufwändig, da hier keine entsprechende Benutzerschnittstelle vorhanden ist.

Fehlende Summenspeicher in der Smartcard

Beschreibung

Im RKS-V-Verfahren werden Summenspeicher von der Registrierkasse verwaltet, demgegenüber werden sie bei INSIKA während der Signaturerstellung automatisch in der Smartcard aktualisiert. Umsatzspeicher in der Registrierkasse sind ohne Zusatzmaßnahmen nicht vertrauenswürdig. Tagesabschlüsse mit verlässlichen Umsatzwerten sind jedoch erforderlich, um Gesamtumsätze für – etwa durch technische Fehler entstandene – Datenlücken dem Grunde und Höhe nach sicher ermitteln zu können.

Ersatzmechanismus

Um ein Entdeckungsrisiko für Manipulation von Summenspeichern zu schaffen, wird ein laufender Gesamtumsatzzähler in jede Signatur einbezogen. Damit diese Daten nicht für jedermann einsehbar sind, werden sie symmetrisch verschlüsselt. Den Schlüssel dazu legt der Steuerpflichtige selbst fest und übermittelt ihn online an die Finanzverwaltung.

Bewertung

Über den Umsatzzähler wird offensichtlich nur der Gesamtumsatz abgesichert. Verschiebungen zwischen Umsatzsteuersätzen in den Summenspeichern wären bei Vernichtung eines Teils der Detailaufzeichnungen (als Begründung können technische Fehler vorgeschoben werden) nicht erkennbar.

Erfolgt eine Manipulation, indem eine große Buchung produziert, deren Beleg vernichtet, die Buchung storniert wird und anschließend die Daten der Buchung sowie der Stornierung gelöscht werden (z.B. unter Vorspiegelung eines technischen Fehlers), ist das bei INSIKA am Summenspeicher für Negativbuchungen sicher erkennbar. Beim RKS-V-Verfahren ist ein Summenspeicher für Negativbuchungen nicht vorgesehen. Dieser Angriff ist praktisch natürlich nicht allzu häufig durchführbar – die Sicherheit bleibt hier aber hinter dem INSIKA-Verfahren zurück.

Wird der Schlüssel für den Umsatzzähler kompromittiert (etwa im Rahmen der Übermittlung an die Finanzverwaltung oder per Auslesen aus der Registrierkasse durch Mitarbeiter), ist der bisherige Umsatz der Registrierkasse aus jedem Beleg ersichtlich. Falls mehrere Belege vorhanden sind, ist der Umsatz zwischen jeweils zwei Belegen durch einfache Differenzbildung ermittelbar. Ein frei durch den Anwender wählbarer Schlüssel führt sehr oft nicht zu Wahl „starker“ Passwörter, erfolgreiche Wörterbuchangriffe sind dadurch wahrscheinlich. Durch die Darstellung des Umsatzzählers mit vollen Hunderten ist er bei einem kleinen Verkaufsbetrag mit sehr großer Wahrscheinlichkeit identisch zum vorherigen Beleg. Dadurch wird ein Ciphertext-Only-Angriff stark erleichtert. Auch durch Salt (Aufnahme von Zufallsziffern in die zu verschlüsselnden Daten) ist das nicht zu verhindern.

Speicherung sicherheits- und signaturrelevanter Daten in der Kasse statt in der Smartcard

Beschreibung

Summenspeicher, fortlaufende Belegnummer, Kassenidentifikationsnummer und der Signaturwert des vorgehenden Barumsatzes werden in der Kasse gespeichert. Hier sind sie einem Risiko un-

berechtigter Veränderung und/oder technischen Problemen ausgesetzt.

Ersatzmechanismus

Belegverkettung und fortlaufender, verschlüsselter Gesamtumsatzzähler (wie oben beschrieben).

Bewertung

Alle Daten in der Kasse sind grundsätzlich nicht vertrauenswürdig. Da die Ersatzmechanismen (Belegverkettung durch Signaturwert, Umsatzzähler als Teil der Signatur) nicht alle Angriffsszenarien abdecken, verbleiben Sicherheitsrisiken. Eine vollständige Analyse ist hier nicht möglich und beabsichtigt, daher sei nur ein Beispiel genannt:

Der Signaturvorgang eines Barverkaufs hinterlässt „Spuren" ausschließlich in Belegen und aufgezeichneten Daten, nicht aber in der Smartcard (diese ist ja eine Standard-Signaturkarte ohne die funktionalen Erweiterungen einer INSIKA-Karte). Gelangt der letzte Beleg nach der verpflichtenden Belegausgabe wieder in den Besitz des Kassenbetreibers (z.B. zurückgelassene Rechnung im Restaurant), lässt sich der Barverkauf spurlos entfernen (Löschen aus den aufgezeichneten Daten, Rücksetzen von Sequenzzähler, Umsatzzähler und Signaturwert zur Belegverkettung). Dieser Angriff ist auch mit einer lückenlosen Kette mehrerer Belege möglich. Erst wenn ein Beleg das Haus tatsächlich verlassen hat, ist diese Manipulation für zuvor erstellte Belege nicht mehr unerkannt möglich. Der wesentliche Unterschied zum INSIKA-Verfahren liegt darin, dass die Entscheidung zur Manipulation nach der Belegerstellung getroffen werden kann, während sie bei der Nutzung von INSIKA vor der Belegerstellung fallen müsste. Das Entdeckungsrisiko ist damit wesentlich reduziert.

Eine Reihe praktischer Probleme ergibt sich, sobald Inkonsistenzen zwischen Smartcard, Datenerfassungsprotokoll und weiteren Daten in der Kasse entstehen – beispielsweise als Folge von Datensicherungen/-rücksicherungen im Falle von Defekten. Dann treten sowohl inkonsistente Verkettungen von Signaturen als auch fehlerhafte Belegnummern auf (entweder lückenhafte oder doppelte Nummern). Damit kann zwar die Finanzverwaltung einen Fehler nachweisen, es gibt aber keinerlei Hilfestellung für den Steuerpflichtigen, die Auswirkungen des Fehlers zu begrenzen. Bei INSIKA führt die absolut eindeutige Kennzeichnung eines jeden Belegs durch Steuernummer, Kartennummer und Sequenznummer – die unabhängig ist von allen äußeren Faktoren und von vorherigen Belegen – zu wesentlich besseren Möglichkeiten, defekte Datenbestände weitgehend und vor allem transparent zu „reparieren".

Kein steuerliches Identifikationsmerkmal in der Smartcard

Beschreibung

Bei INSIKA ist das Identifikationsmerkmal des Steuerpflichtigen auf der Smartcard abgelegt und fließt direkt in die Signatur ein. So ist ein unmittelbarer Rückschluss vom Beleg auf die Smartcard und weiter auf den Steuerpflichtigen möglich.

Ersatzmechanismus

Im RKS-V-Verfahren wird dies durch einen komplexen Mechanismus bestehend aus Kassenidentifikationsnummer, Seriennummer des Zertifikats, Global Location Nummer und einer Datenbank über die Sicherheitseinrichtungen ersetzt.

Bewertung

Die komplexen Strukturen erschweren die Nachvollziehbarkeit und bedingen speziell in Fehlersituationen einen erhöhten Aufwand. Besonders beim Austausch von Geräten, z.B. bei Defekten oder Umsetzungen zwischen Filialen gibt es zusätzliche, fehlerträchtige Arbeitsschritte.

Keine Lösung für Agentur- und Lieferscheinumsätze

Beschreibung

INSIKA erlaubt die Abbildung von Agenturgeschäften (also von Geschäften im Namen Dritter beispielsweise beim Verkauf von Kraftstoffen) sowie Lieferscheinen (es wird ein Beleg ausgegeben, die Rechnungsstellung erfolgt aber über ein separates Verfahren außerhalb der Kasse). Die Absicherung bei Datenverlusten erfolgt über die Summenspeicher/Tagesabschlüsse. Im RKS-V-Verfahren gibt es keine vollwertige Entsprechung, da dies abgesicherte Summenspeicher auch für Agentur- und Lieferscheinumsätze erfordern würde.

Ersatzmechanismus

Keiner.

Bewertung

Agentur- und Lieferscheingeschäfte kommen in der Praxis nicht selten vor, so dass hierfür eine Lösung gefunden werden muss. Spätestens bei Fehlern (z.B. Teilverlusten von aufgezeichneten Daten) wird es aufgrund fehlender detaillierter und sicherer Tagesabschlüsse Probleme mit der Nachvollziehbarkeit geben.

Deutlich mehr und größere signaturrelevante Daten auf dem Beleg

Beschreibung

Durch die Verwendung zweier Identifikationsnummern (Kassenidentifikationsnummer und Seriennummer des Zertifikats), des verschlüsselten Umsatzzählers (durch die AES-Blockgröße von 128 Bit 16 Bytes lang, also 24 Zeichen in einer Base64-Codierung) und des Signaturwerts des vorhergehenden Datensatzes sind die Daten zur Signaturverifikation sehr umfangreich. Ein Ausdruck im Klartext auf dem Beleg ist also äußerst unhandlich. Damit ist die Verwendung eines 2D-Codes nahezu zwingend. Weiter verschärft würde das bei der (offenbar zulässigen) Verwendung von RSA- statt ECDSA-Signaturen (schon bei 1024 Bit Schlüsseln ist allein die Signatur 128 Bytes lang).

Ersatzmechanismus

Keiner.

Bewertung

Durch den Zwang, einen 2D-Code zu drucken ist die Nachrüstbarkeit bestehender Systeme erheblich eingeschränkt bzw. die Nachrüstung wird in vielen Fällen deutlich verteuert. Eine Übergangsregelung, die auch einen Ausdruck der signaturrelevanten Informationen im Klartext erlaubt, ist aufgrund der Datenmengen in der Praxis deutlich schwieriger zu handhaben als beim INSIKA-Verfahren.

Formulierung von Anforderungen an die Registrierkasse

Beschreibung

Beim INSIKA-Verfahren werden lediglich Anforderungen an Daten und Belege gestellt. Das RKS-V-Verfahren formuliert dagegen ausdrücklich Anforderungen an die Registrierkasse.

Ersatzmechanismus

Keiner.

Bewertung

Die Einhaltung der Anforderungen kann zu großen Teilen – wie beim INSIKA-Verfahren – durch eine Kontrolle von Belegen und die Prüfung der aufgezeichneten Daten verifiziert werden. Dies gilt jedoch nicht für alle Anforderungen wie beispielsweise die korrekte Funktion der Summenzähler. Hier entstehen nicht nur Sicherheitsrisiken sondern auch Haftungs- bzw. Gewährleistungsrisiken für Hersteller und Anwender.

Würden zur Erhöhung der Sicherheit Zertifizierungsverfahren, Konformitätserklärungen der Hersteller o.ä. eingeführt, hätte das erhebliche Auswirkungen auf den finanziellen und den Zeitaufwand bei der Entwicklung von Registrierkassen. Jede Softwareänderung würde eine Rezertifizierung erforderlich machen.

Eine flächendeckende Marktaufsicht mit technisch entsprechend spezialisierten Fachkräften ist mit vertretbarem Aufwand kaum vorstellbar.

Weitere Aspekte

Neben den rein technischen Aspekten gibt es beim RKS-V-Verfahren einige weitere Punkte, die ebenfalls deutliche Nachteile mit sich bringen.

Preise von Standard-Signaturkarten

Beschreibung

Mit der Wahl von Standard-Signaturkarten könnte sich die Erwartung verbinden, dass der Wettbewerb für besonders günstige Preise sorgt.

Bewertung

Aufgrund der rechtlichen Rahmenbedingungen, der sich daraus ergebenden Prozesse (z.B. zur Identitätsfeststellung) und der relativ kleinen Stückzahlen sind die Kosten für Standard-Signaturkarten für qualifizierte elektronische Signaturen grundsätzlich höher als bei Smartcards für das INSIKA-Verfahren. Daran kann und wird auch der Wettbewerb verschiedener Anbieter nichts ändern.

Qualifizierte elektronische Signaturen nur für natürliche Personen

Beschreibung

Nach aktueller Rechtslage können qualifizierte Zertifikate nur für natürliche Personen ausgestellt werden. Entsprechende Signaturkarten erfordern i.d.R. eine PIN-Eingabe vor jedem Signaturvorgang.

Bewertung

Bargeschäfte werden in vielen Fällen von juristischen Personen (also z.B. Kapitalgesellschaften) getätigt. Es ist daher systematisch wenig sinnvoll, in diesen Fällen die Zertifikate für natürliche Personen auszustellen.

Durch die eIDAS-Veordnung, die am 1. Juli 2016 in Kraft tritt, kann ein „qualifiziertes elektronisches Siegel“ verwendet werden, was die beschriebenen Probleme löst. Allerdings müssen die

erforderlichen Produktentwicklungen bereits vorher erfolgen.

Speicherung der Daten in der Registrierkasse

Beschreibung

Der Wortlaut der RKS-V ist so auslegbar, dass alle erfassten Daten für die gesamte Aufbewahrungsfrist in der Registerkasse zu speichern sind.

Bewertung

Diese Anforderung wäre nicht praktikabel. Selbst wenn der nötige Speicher zur Verfügung steht, ist in vielen Betrieben eine zentrale Speicherung und Verwaltung das einzig sinnvolle Vorgehen.

Entwicklung des Konzepts nicht in einem strukturierten Projekt

Beschreibung

Aus der Tatsache, dass der Verordnungsentwurf innerhalb kurzer Zeit entstanden ist und keine weitergehende Dokumentation vorliegt, lässt sich unschwer folgern, dass das beschriebene Verfahren nicht das Ergebnis eines zielgerichteten Entwicklungsprojekts sein kann. INSIKA wurde nach einer mehrjährigen Konzeptphase von einem Projektkonsortium über einen Zeitraum von vier Jahren spezifiziert, getestet und dokumentiert. Als Ergebnis liegt umfangreiche Dokumentation einschließlich technischer Spezifikationen und Darstellung der Sicherheitsmechanismen vor. Die Dokumentation wurde inzwischen von einer Vielzahl von Experten geprüft. INSIKA wird zudem erfolgreich in der Praxis eingesetzt.

Bewertung

Ein komplexes Sicherheitsverfahren, das nicht im Rahmen eines größeren Projekts entwickelt und keinerlei praktischer Erprobung unterzogen wurde, birgt ein erhebliches Risiko konzeptioneller Schwächen und Sicherheitslücken (bereits diese kurze Analyse hat die ersten Lücken aufgedeckt). Erfahrungsgemäß führt das zu Nachbesserungen, die erhebliche Kosten für Systemhersteller, Anwender und Finanzbehörden verursachen können. Aufgrund der kurzen Fristen ist ein wirklicher Praxistest nicht durchführbar, so dass von der Theorie unmittelbar in den Echtbetrieb übergegangen werden muss.

Meldepflicht für Ausfälle (nicht nur bei Verlust einer Smartcard)

Beschreibung

Die Verordnung sieht vor, dass Ausfälle einer Registrierkasse oder eine Außerbetriebnahme anzeigepflichtig sind. Diese Vorgabe hat allerdings keinen Bezug zum gewählten technischen Verfahren.

Bewertung

Diese Anforderung kann erheblichen Aufwand beim Betreiber erzeugen – in einer Situation, in der es vor allem darum gehen wird, den Geschäftsbetrieb aufrecht zu erhalten.

Ausnahmeregelung für geschlossene Systeme

Beschreibung

Die RKS-V sieht eine Ausnahmeregelung vor, nach der Großunternehmen mit sog. „geschlossenen Gesamtsystemen“ nicht zum Einsatz von Smartcards verpflichtet werden. Eine kryptografische Sicherung der Daten ist allerdings trotzdem vorgeschrieben. Die Ordnungsmäßigkeit des Systems ist durch ein Sachverständigengutachten nachzuweisen. Über technische Maßnahmen (etwa Hashwerte für Softwaremodule) muss bei einer Prüfung nachgewiesen werden können, dass das System mit dem im Gutachten beschriebenen identisch ist.

Bewertung

Sinnvoll wäre eine derartige Ausnahmeregelung nur dann, wenn in einem Großbetrieb keinerlei Veränderungen an den Registrierkassen erforderlich wären, sondern ausschließlich zentrale Komponenten angepasst werden müssten – die Kosten einer Umstellung entstehen vor allem für Veränderungen an den Registrierkassen. Da auch bei Großunternehmen mit „geschlossenen Systemen“ die Registrierkassen das geforderte Signaturverfahren (wenn auch ohne Nutzung einer Smartcard) implementieren und 2D-Codes drucken müssen, fallen auch hier die Umstellungskosten für Registrierkassen fast in voller Höhe an.

Zudem sind die Anforderungen an das zu erstellende Gutachten offensichtlich derart hoch, dass hier in jedem Fall mit erheblichen Kosten gerechnet werden muss – wenn sich überhaupt geeignete Sachverständige finden lassen. Dass sich versteckte Manipulationsfunktionen in so einem Verfahren kaum entdecken ließen, dürfte allerdings das wesentliche Problem sein.

Die Absicherung von Softwarewaremodulen in einem komplexen, oft heterogenen System ist äußerst schwierig. Wesentlich kritischer ist hier jedoch, dass Softwareupdates ganz erheblich erschwert werden, da sie systemimmanent mit einer erneuten Prüfung verbunden sind.

Insgesamt erscheint die Ausnahmeregelung deshalb völlig praxisfern.

Fazit

Das im Entwurf der Registrierkassensicherheits-Verordnung vom 30. Juni 2015 beschriebene Verfahren ist an INSIKA angelehnt, jedoch in zentralen, sicherheitsrelevanten Punkten stark verändert.

Das daraus resultierende Verfahren ist gegenüber INSIKA weniger sicher, weniger robust bei Fehlern und zudem teurer. Es erzeugt Mehraufwand sowohl bei Herstellern und Anwendern als auch bei den Finanzbehörden. Bei technischen Störungen verschlechtern sich die Nachweismöglichkeiten der Anwender gegenüber der Finanzverwaltung. Eine wesentliche Sicherheitslücke ist in diesem Dokument beschrieben. Auf die Beweiskraft des Verfahrens – speziell die für den Steuerpflichtigen gegenüber der Finanzverwaltung – können Sicherheitslücken nur negative Auswirkungen haben.

Auch durch Nachbesserungen am Verfahren sind die wesentlichen Probleme nicht zu beseitigen, da sie durch die grundsätzlichen Strukturen verursacht werden.

Die Erleichterungen für Großunternehmen mit „geschlossenen Systemen“ sind an derart hohe Voraussetzungen geknüpft, dass sie praktisch kaum nutzbar sind.

Kontakt

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

www.insika.de

E-Mail: info@insika.de