INSIKA®: Kryptografischer Manipulationsschutz für Registrierkassen und Taxameter

Analyse der österreichischen Registrierkassen-sicherheitsverordnung vom 11. Dezember 2015

Stand: 30. März 2016

Das österreichische Steuerreformgesetz 2015/2016 beinhaltet eine Registrierkassen- und Belegpflicht sowie die Verpflichtung zum Einsatz einer technischen Manipulationssicherung. Diese wird in der Registrierkassensicherheitsverordnung vom 11. Dezember 2015 sowie deren Anlagen spezifiziert.

Das gewählte Verfahren nutzt Grundideen von INSIKA, 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 dieser Nachteile treffen die Anwender. Mehrere Sicherheitslücken – davon eine erhebliche – sind in dieser Analyse dargestellt. Sie waren bereits in der Begutachtungsphase bekannt. Die Beweiskraft eines Sicherheitssystems mit bekannten, wesentlichen Schwächen ist fraglich.

Für sog. geschlossene Gesamtsysteme 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.

In dieser aktualisierten Version der Analyse sind Erkenntnisse aus den letzten Monaten und aus der praktischen Umsetzung eingeflossen.

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 zu etablieren – und dabei vor allem eine echte Alternative zu konventionellen, sehr aufwändigen „Fiskalkassensystemen“ zu bieten. Ein besonderer Schwerpunkt ist die Rechtssicherheit für die Anwender der Systeme.

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.[1] Die weiteren Details werden durch die Registrierkassensicherheitsverordnung (RKSV) bestimmt. Die in diesem Dokument analysierte Endfassung der Verordnung[2] wurde am 11. Dezember 2015 veröffentlicht und ist identisch zum Entwurf vom 1. September, der dann im Verfahren gemäß EU-Richtlinie 98/34/EG notifiziert wurde. Die Endversion entspricht weitgehend dem Begutachtungsentwurf vom 30. Juni 2015.

[1] Online abrufbar unter http://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2015_I_118/BGBLA_2015_I_118.pdf

[2] Online abrufbar unter http://www.bmf.gv.at/steuern/BGBLA_2015_II_410.pdf

Die genaue Entstehungsgeschichte der RKSV sowie eine Anforderungsspezifikation für das RKSV beschriebene Verfahren (im Folgenden „RKSV-Verfahren“) ist dem ADM e.V. nicht bekannt. Es liegt aber die Vermutung nahe, dass es Ziel der RKSV 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 dabei exakt auf die Anforderungen abgestimmt. Alle wesentlichen Sicherheitsfunktionen laufen kartenintern ab, also ohne die Möglichkeit einer Beeinflussung von außen. Der Verzicht auf spezielle Smartcards beim RKSV-Verfahren führt zu erheblichen Unterschieden gegenüber einer Lösung nach dem INSIKA-Verfahren. 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 der Signatur der vorherigen Buchung (technisch erfolgt das in Form eines Hashwertes). Bei der ersten Buchung ist ein aus der Kassenidentifikationsnummer berechneter Initialwert zu verwenden.

Bewertung

Auf den ersten Blick erfüllt das Verfahren den Zweck. Es bleiben jedoch Sicherheitslücken. Zudem ist das System bei Störungen weniger robust als das INSIKA-Verfahren. Beide Aspekte sind im Abschnitt „Speicherung sicherheits- und signaturrelevanter Daten in der Registrierkasse statt in der Smartcard“ erläutert.

Fehlende Summenspeicher in der Smartcard

Beschreibung

Im RKSV-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. Zwischenabschlüsse mit verlässlichen Umsatzwerten sind jedoch erforderlich, um Gesamtumsätze für – etwa durch technische Fehler entstandene – Datenlücken dem Grunde und der 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 mit dem AES-Algorithmus symmetrisch verschlüsselt. Den Schlüssel dazu legt der Steuerpflichtige selbst fest und übermittelt ihn online an die Finanzverwaltung.

Bewertung

Über den Umsatzzähler wird 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 durchgeführt, 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 RKSV-Verfahren ist ein Summenspeicher für Negativbuchungen nicht vorgesehen. Dieser Angriff ist in der Realität 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 wahrscheinlicher. Wenn der Benutzer nicht sicherstellt, dass die Kombination aus AES-Schlüssel, Kassen-ID und Belegnummer nicht mehrfach vorkommt, ergeben sich daraus Angriffsmöglichkeiten.

Die Übermittlung eines über 40 Zeichen langen Schlüssels (256 Bit als Base64 codiert) an die Finanzverwaltung ist unkomfortabel und fehlerträchtig.

Darüber hinaus ist unklar, warum zugunsten von Monats- und Jahresabschlüssen auf Tagesabschlüsse, die vor allem mehr Sicherheit für den Anwender bei technischen Fehlern bedeuten, verzichtet wurde.

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

Beschreibung

Summenspeicher, fortlaufende Belegnummer, Kassenidentifikationsnummer und der Signaturwert des vorgehenden Barumsatzes werden in der Registrierkasse gespeichert. Hier sind sie einem Risiko unberechtigter Veränderung und/oder technischen Problemen ausgesetzt.

Ersatzmechanismus

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

Bewertung

Alle Daten in der Registrierkasse sind grundsätzlich nicht vertrauenswürdig. Da die Ersatzmechanismen (Belegverkettung durch Signaturwert, Umsatzzähler als Teil der Signatur) nicht alle Angriffsszenarien abdecken, verbleiben Sicherheitsrisiken. Interessanterweise wird die Erweiterung der Software einer Standard-Smartcard (die ja auch evaluierbar ist) gegenüber der Verlagerung von Sicherheitsmechanismen in die Kasse als weniger sicher angesehen.[3]

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 ohne Entdeckungsrisiko 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 Registrierkasse 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 bes-

[3] Vgl. http://www.globaltrust.eu/static/rksv-posch-20150917.pdf

seren 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 RKSV-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. So gibt es keinen Schutz gegen versehentlich falsch eingegebene oder doppelt genutzte Kassenidentifikationsnummern.

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 Registrierkasse). Die Absicherung bei Datenverlusten erfolgt über die Summenspeicher/Tagesabschlüsse. Im RKSV-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[4] 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 verpflichtende Verwendung eines 2D-Codes praktisch zwingend und folgerichtig auch in der Verordnung verankert. Weiter verschärft würde das bei der (offenbar zulässigen) Verwendung von RSA- statt ECDSA-Signaturen (bei dem Stand der Technik entsprechenden 2048-Bit-Schlüsseln ist allein die Signatur schon 256 Bytes lang, selbst bei 1024-Bit-Schlüsseln sind es noch 128 Bytes).[5]

Ersatzmechanismus

Die Verordnung erlaubt alternativ den Druck der Daten in OCR-A-Schrift oder als Link auf eine Website.

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, wäre aufgrund der Datenmengen in der Praxis deutlich schwieriger zu handhaben als beim INSIKA-

[4] In älteren Fassungen dieser Analyse ist davon ausgegangen worden, dass der verschlüsselte Umsatzzähler immer 16 Bytes lang ist. Aus der inzwischen vorliegenden Detailspezifikation (Anlage zur RKSV) geht hervor, dass der Counter-Mode verwendet wird, was zu 5 Bytes großen Zählern führt. An der Gesamtbeurteilung ändert das jedoch nichts.

[5] Die beiden angebotenen Signaturkarten verwenden allerdings sinnvollerweise ECDSA.

Verfahren – folgerichtig gibt es auch keine Übergangsregelung.

Der Druck der Daten in OCR-A-Schrift wird mit den meisten Druckern, die keine QR-Codes darstellen können, ebenfalls nicht möglich sein.

Das Ablegen von Beleginformationen auf einem Webserver stellt eine weitere potenzielle Sicherheitslücke dar. Hiermit ist es möglich, den Signaturvorgang erst beim Abruf durchzuführen. Die Forderung der sofortigen Signatur und der damit verbundenen Festschreibung der Daten kann damit unterlaufen werden.

Formulierung von Anforderungen an die Registrierkasse

Beschreibung

Beim INSIKA-Verfahren werden lediglich Anforderungen an Daten und Belege gestellt. Das RKSV-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 Neuzertifizierung erforderlich machen.[6]

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

[6] Entsprechende Bestrebungen des Gesetzgebers sind aktuell allerdings nicht bekannt.

Weitere Aspekte

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

Qualifizierte elektronische Signaturkarten nicht geeignet

Beschreibung

Nach aktueller Rechtslage können qualifizierte Zertifikate nur für natürliche Personen ausgestellt werden. Entsprechende Signaturkarten erfordern 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. Die PIN-Eingabe muss durch eine Speicherung der PIN in der Registrierkasse umgangen werden.

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.

Die praktische Lösung besteht darin, Karten für qualifizierte elektronische Signaturen zu verwenden, diese allerdings nicht wie vorgesehen zu betreiben. Die Zertifikate werden also auch für juristische Personen ausgestellt und die PIN-Nummer muss in der Kasse gespeichert und für jede Signatur gesendet werden.

Datenexportformat nicht vollständig

Beschreibung

Das dokumentierte Datenexportformat für das Datenerfassungsprotokoll beinhaltet nur Gesamtsummen jedes Verkaufsvorgangs (und die kryptografischen Daten) aber nicht die Detailpositionen.

Bewertung

Dies erfordert die Bereitstellung von Daten in zwei verschiedenen Formaten, da die Detailinformationen nach wie vor Inhalt der Prüfung sein werden. Für die Detaildaten ist aber weiterhin kein eindeutiges Format definiert, so dass ein Ende der Auseinandersetzungen zwischen Steu-

erpflichtigen und Finanzverwaltung über die Auswertbarkeit nicht abzusehen ist. Die Prüfung von Daten, die zusammengehören aber auf zwei Wegen übertragen werden, wirft eine Reihe praktischer Probleme auf.

Speicherung der Daten in der Registrierkasse

Beschreibung

Der Wortlaut der RKSV 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 Verfahrens nicht in einem strukturierten Projekt

Beschreibung

Aus der Tatsache, dass die Verordnung innerhalb weniger Wochen entstanden ist und zum Zeitpunkt der Veröffentlichung keine weitergehende Dokumentation vorlag, lässt sich nur 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 Einführungsfristen ist ein wirklicher Praxistest nicht mehr durchführbar, so dass von der Theorie unmittelbar in den Echtbetrieb übergegangen werden muss. Die bisherigen Erfahrungen bei der Umsetzung bestätigen, dass viele Unklarheiten nachträglich beseitigt werden mussten.

Wenig Entwicklungsunterstützung vorhanden

Beschreibung

Mit der Veröffentlichung des Entwurfs der Verordnung mussten sofort die Implementierungsarbeiten bei den Herstellern beginnen, damit noch Chancen bestehen, die Frist bis 1.1.2017 einzuhalten. Eine (noch unvollständige) Referenzimplementierung und Beispieldaten standen erst ab Oktober 2015 zur Verfügung.

Bewertung

Das Erfordernis, ein bisher nur theoretisch existierendes, komplexes Verfahren unter hohem Zeitdruck fehlerfrei zu implementieren, bringt erhebliche Kosten- und Terminrisiken mit sich. Die Folgen tragen Hersteller und Anwender.

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 RKSV sieht eine Ausnahmeregelung vor, nach der mittlere und große Unternehmen 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 Maß-

nahmen (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 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 „geschlossenen Gesamtsystemen" 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. Softwareupdates werden ganz erheblich erschwert, da sie systemimmanent mit einer erneuten Prüfung verbunden sein müssten. In den Erläuterungen zur Verordnung wird allerdings darauf hingewiesen, dass Software-Updates, welche nicht die Sicherheitseinrichtung betreffen, ohne erneute Prüfung möglich sind – einen Nutzen haben die geforderten Hashwerte für Softwaremodule damit allerdings nicht mehr.

Insgesamt erscheint die Ausnahmeregelung unausgereift und praxisfern.

Fazit

Das in der Registrierkassensicherheits-Verordnung vom 11. Dezember 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.

Alle wesentlichen Probleme sind systembedingt und daher nicht durch kleinere Anpassungen nachträglich zu beseitigen.

Die Erleichterungen für „geschlossene Gesamtsysteme" 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

Praktische Erfahrungen bei der Umsetzung

Bei der Implementierung der Anforderungen der RKSV durch verschiedene Entwickler hat sich bestätigt, dass die fehlende Praxiserprobung des Verfahrens zu einer Reihe von Unzulänglichkeiten geführt hat.

Im Folgenden sind die wesentlichen Punkte aufgeführt (ohne Anspruch auf Vollständigkeit, aber sicher durchaus repräsentativ):

Verschiedene Karten sind nicht kompatibel

Die Karten der beiden Anbieter haben kein einheitliches Protokoll und müssen mit einem unterschiedlichen Befehlssatz angesprochen werden.

Jeder neue Anbieter oder auch Änderungen an den Signaturkarten der bisherigen Anbieter ziehen eine Änderung der Kassensoftware nach sich. Bereits in der Entwicklungsphase hat es solche inkompatiblen Änderungen bei einem der Anbieter gegeben.

Zertifikatskette muss ins DEP

Ohne ersichtlichen technischen Grund fordert die RKSV, dass die gesamte Zertifikatskette in das Datenerfassungsprotokoll geschrieben werden muss. Root- und Zwischenzertifikate könnten problemlos in der Verifikationssoftware abgelegt werden.

Die Zertifikate sind nur bei einem der beiden Kartenanbieter auf der Karte enthalten. Beim anderen Anbieter müssen sie auf anderen Wegen in die Kasse geladen werden – das bedeutet für Systeme, die nicht PC-basiert und nicht mit Internet verbunden sind, einen nennenswerten Zusatzaufwand sowie eine potenzielle Fehlerquelle.

Doppelte Personalisierung

Es muss sowohl die Smartcard auf den Steuerpflichtigen personalisiert werden als auch eine Online-Registrierung bei FinanzOnline durchgeführt werden. Das ist speziell bei einer größeren Anzahl von Kassen aufwändig, da recht viele Daten bei der Registrierung erfasst werden müssen.

Benachteiligung von Entwicklern, die nicht mit Java arbeiten

Wenn keine Java-Standardbibliotheken vorhanden sind, wird die Entwicklung deutlich aufwändiger.

So sind z.B. alle Strings als UTF-8 codiert, es wird JWS (JSON Web Signature) verwendet und Datenerfassungsprotokoll wird im JSON-Format erzeugt.

Spezifikationslücken nicht geschlossen

Viele Details sind nicht oder nicht sauber spezifiziert. Statt einer Anpassung der Spezifikation werden diese Details per Mustercode bzw. in Readme und FAQs des A-SIT „definiert“.

Beispiele: Markierung von Storno- oder Trainingsbelegen, Erzeugen der JWS-Signatur, Verhalten der Kasse, wenn die Signaturkarte ausgefallen ist.

Unklare Support-Kanäle

Es erfolgt zwar eine unbürokratische Unterstützung durch A-SIT, es ist aber kein offizieller Ansprechpartner für Support vorhanden. Insbesondere bei Regelungslücken der Verordnung und fachlichen Unklarheiten ist das ein Problem.

Demokarten und Demo-Programmcode zu spät verfügbar

Erst ein gutes Jahr vor Start des Echtbetriebs waren die unbedingt nötigen Werkzeuge für Entwickler verfügbar (in dem Zeitraum müssen Entwicklung und Roll-out abgeschlossen werden).

Nur rudimentäre Verifikationssoftware

Es gibt eine nur Kommandozeilen-Verifikationssoftware als Java-Package. Sie ist damit nur zur Überprüfung einer Implementierung durch Entwickler geeignet. Eine Verifikation beim Anwender der Registrierkasse ist damit nicht praktikabel.