INSIKA®: Kryptografischer Manipulationsschutz für Registrierkassen und Taxameter

Whitepaper: Zeitinformationen beim Manipulationsschutz für Registrierkassen

Stand: 31. Mai 2018

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 und ähnliche Geräte eingesetzt werden.

Grundsätzlich ist eine auf dem INSIKA-Verfahren basierende Signaturstellungseinheit geeignet, als Sicherheitsmodul gemäß der Kassensicherungsverordnung (KassenSichV) zu fungieren. Die KassenSichV fordert allerdings einen anderen Umgang mit Zeitinformationen als er in der aktuellen INSIKA-Spezifikation implementiert ist.

Dieses Whitepaper diskutiert die Auswirkungen und die praktische Umsetzbarkeit einer Zeitquelle im Sicherheitsmodul im Allgemeinen sowie spezifisch für das INSIKA-Verfahren. Es wird eine einfach umsetzbare Erweiterung der INSIKA-Spezifikation vorgestellt.

Für ein hochsicheres und gleichzeitig preiswertes Sicherheitsmodul kommt nach heutigem Stand der Technik nur eine Smartcard in Frage. Smartcards mit Zeitgeber sind angekündigt, jedoch noch nicht verfügbar.

Grundsätzliches

Gemäß § 146a der Abgabenordnung (AO) müssen Registrierkassen ab dem 1. Januar 2020 eine technische Sicherheitseinrichtung (bestehend „aus einem Sicherheitsmodul, einem Speichermedium und einer einheitlichen digitalen Schnittstelle“) verwenden.

Die KassenSichV[1] definiert einige konkretere Anforderungen, ist in weiten Teilen jedoch genauso allgemein gehalten wie das Gesetz.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) arbeitet im Auftrag des Bundesministeriums der Finanzen (BMF) darauf basierende technische Richtlinien und Schutzprofile aus. Diese liegen ausschließlich im Entwurf vor und sind bisher nur zum Teil öffentlich verfügbar.

Während eine Signaturerstellungseinheit auf Basis des INSIKA-Verfahren fast alle Voraussetzungen der KassenSichV für ein Sicherheitsmodul erfüllt, lässt sich die folgende Anforderung aus § 2 nicht ohne weiteres umsetzen:

Die Zeitpunkte nach Satz 2 Nummer 1 und 6 [also Zeitpunkt des Vorgangsbeginns, Zeitpunkt der Vorgangsbeendigung oder des Vorgangsabbruchs], [...] werden manipulationssicher durch das Sicherheitsmodul festgelegt.

Begriffe

In diesem Whitepaper wird der Begriff **Sicherheitsmodul** so verwendet wie in der KassenSichV definiert – also als zentrale und besonders abgesicherte Komponente der Sicherheitseinrichtung.

Verfügt das Sicherheitsmodul über einen eigenen Zeitgeber (unabhängig von der Frage, wie dieser auf die korrekte Zeit eingestellt wird) und fügt den Transaktionen automatisch Datum und Uhrzeit hinzu, wird das als **interne Zeitquelle** bezeichnet. Stammt die Uhrzeit jeder Transaktion vom Host-System (also z. B. der Registrierkasse) wird es **externe Zeitquelle** genannt.[2]

Eine **Transaktion** ist jeder Vorgang, der von der Sicherheitseinrichtung geschützt werden soll (genauer: Manipulationen daran sollen erkennbar gemacht werden), in jedem Fall also Verkaufsvorgänge.

Ein **Angriff** ist jede Handlung mit dem Ziel, das Sicherungssystem zu unterlaufen, z. B. durch eine unerkannte Manipulation oder auch durch eine komplette Umgehung des Systems.

[1] Verordnung zur Bestimmung der technischen Anforderungen an elektronische Aufzeichnungs- und Sicherungssysteme im Geschäftsverkehr vom 26.09.2017, http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl117s3515.pdf

[2] Diese Begriffe werden auch im Begründungsteil der KassenSichV (siehe Fußnote 3) verwendet, jedoch nicht klar definiert und offenbar auch in einer anderen Bedeutung.

Sicherheitsaspekte

Begründung der Anforderung

Eine direkt aus dem Sicherungszweck entwickelte Herleitung der Anforderung einer internen Zeitquelle in der KassenSichV gibt es nicht. Im Begründungsteil wurde seinerzeit – nicht einmal direkt zum Thema – ausgeführt:

Die Protokollierung des Zeitpunkts des Vorgangsbeginns soll sicherstellen, dass die Vorfälle zeitnah erfasst werden, aufgrund der Zeitangabe aufgefunden werden können und in endlicher Zeit abgeschlossen werden. Außerdem sollen damit nachträgliche Erfassungen an einer Zweitkasse unterbunden werden.[3]

Unklar bleibt, wie die hier definierten Ziele mittels speziell gesicherter Zeitangaben erreicht werden sollen.

Kontrollen sind entscheidend

In Diskussionen über Sicherungsverfahren kommt immer wieder – meistens nur indirekt formuliert – die prinzipiell nicht erfüllbare Erwartungshaltung auf, dass eine technische Lösung allein für ein sicheres Gesamtsystem sorgen könne.

Eine Nicht- oder Falsch-Erfassung von Transaktionen stellt das Hauptrisiko dar und kann von keinem technischen System eindeutig erkannt oder gar verhindert werden. Es sind also stets begleitende, organisatorische Maßnahmen, vor allem in Form einer flächendeckenden und repräsentativen Feldüberwachung erforderlich.

Eine sinnvolle Sicherheitslösung bewirkt eine „Ende zu Ende"-Absicherung – also vom Moment der Erfassung bis hin zur Prüfung. An beiden „Endpunkten" muss es geeignete Prüfmöglichkeiten geben. Im deutschen Steuerrecht sind das die Kassen-Nachschau und die Außenprüfung.

Bei einer geeigneten Kassen-Nachschau fallen folgende Angriffsversuche auf:

- Nicht-Erfassung,
- Erfassung falscher Daten (z. B. zu geringe Preise),
- Nutzung eines nicht-ordnungsmäßigen Systems (z. B. einer „Zweitkasse", deren Daten nicht in die Buchführung einfließen) oder
- Verwendung falscher Zeitinformationen.

Der Aufwand einer Kassen-Nachschau hängt stark von der gewählten technischen Lösung ab. INSIKA verwendet ein Sicherheitsmerkmal auf dem Beleg (Signatur in numerischer Form oder als QR-Code), das ohne Datenzugriff, also mit in jeder Hinsicht geringstem Aufwand überprüft werden kann.

Nutzen einer internen Zeitquelle

Das folgende Angriffsszenario ist allerdings auch bei effektiven Kontrollen grundsätzlich möglich:

- Transaktionen werden für einen bestimmten Zeitraum nicht an die Sicherheitseinrichtung übergeben, sondern lediglich zwischengespeichert. Das erfolgt mit dem Ziel, die Daten später zu verändern und erst danach – mit den ursprünglichen, also dann falschen Zeitinformationen – an die Sicherheitseinrichtung zu übertragen.
- Hinweis: Damit können allerdings keine korrekten Belege erstellt werden, so dass schon der Verstoß gegen die Belegpflicht auffallen würde.
- Falls eine nicht-verdeckte Kassen-Nachschau stattfindet und in diesem Rahmen ein Beleg verlangt wird, werden die Daten der letzten Transaktionen in korrekter Form nachträglich an die Sicherheitseinrichtung übergeben.
- Hinweis: Dazu müsste das Kassenpersonal zumindest grundsätzlich in die Manipulation eingeweiht sein.
- Beim Abgleich der Daten mit vorher beobachteten Verkäufen würde es keine Auffälligkeiten geben.

Dieses Szenario ist allerdings nicht besonders gut geeignet, um lohnende Manipulationen auszuführen und daher unwahrscheinlich. Durch eine interne Zeitquelle kann es aber verhindert werden. In diesem Sinne erhöht eine interne Zeitquelle die Sicherheit, wenn auch nur in einem geringen Ausmaß.

Anforderung an Zeitquelle aus Sicht von BMF und BSI

Die neueste öffentlich bekannte Auslegung der Anforderungen an die in der KassenSichV geforderte Zeitquelle ist nicht schriftlich dokumentiert, sondern wurde im Rahmen einer Anhörung[4] mündlich erläutert:

[3] Bundestags-Drucksache 18/12221 vom 03.05.2017, http://dipbt.bundestag.de/dip21/btd/18/122/1812221.pdf, Seite 11

[4] Mündliche Anhörung zu den Entwürfen der Technischen Richtlinien des BSI am 27. März 2018 im BMF

- Die Zeitquelle muss nicht batteriegepuffert sein, so dass nach jedem Aus- und Einschalten der Sicherheitseinrichtung ein erneutes Einstellen der Uhrzeit erforderlich ist.
- Die interne Zeitquelle kann durch das Hostsystem ohne besondere Anforderungen an die Zuverlässigkeit der Zeitinformation gesetzt werden.
- Das Setzen der Zeit muss dokumentiert werden, so dass jede Veränderung der Zeit nachvollziehbar ist.

Verfügbarkeit geeigneter Hardware

Grundsätzlich ist es möglich, ein Sicherheitsmodul mit einer internen Zeitquelle in der beschriebenen Form neu zu entwickeln. Der finanzielle und der Zeitaufwand sind aufgrund der erforderlichen Zertifizierung (Common Criteria EAL 4+)[5] sehr hoch.

Aus diesen Gründen ist die Nutzung einer zertifizierten Smartcard als Sicherheitsmodul naheliegend. Ein voraussichtlich geeigneter Zeitgeber ist in der Version 3.1 des JavaCard-Standards vorgesehen.[6]

Smartcards auf dieser Basis sind jedoch momentan noch nicht auf dem Markt erhältlich. Verlässliche Angaben zur voraussichtlichen Verfügbarkeit liegen noch nicht vor.

Erfassung von Vorgangsbeginn und -abbruch

Abgesehen davon, dass noch gar nicht definiert ist, was ein „Vorgang“ ist, existiert keine nachvollziehbare Begründung für eine Aufzeichnungspflicht des Vorgangsbeginns oder eines Vorgangsabbruchs.

Die zugrunde liegende Vorstellung ist offenbar, dass ein Angriff etwa in folgender Art ablaufen könnte:

- Es erfolgen Eingaben an einer Kasse, evtl. auch in Verbindung mit einem Ausdruck, die den Kunden dazu veranlassen, eine Zahlung vorzunehmen.
- Dieser Vorgang wird nicht korrekt abgeschlossen, also nicht an die Sicherheitseinrichtung übergeben.
- Die Zahlung ist damit nicht erfasst.

Dies ist jederzeit daran erkennbar, dass gar kein oder kein korrekter (also von der Sicherheitseinrichtung erfasster) Beleg ausgegeben wurde.

Es ist unklar, warum die Zeit des Vorgangsbeginns oder eines -abbruchs bei der Erkennung des Angriffs helfen sollte. Und warum sollte ein System mit Manipulationsfunktionen im Falle einer Manipulation den Vorgangsbeginn korrekt aufzeichnen und damit eine Entdeckung erleichtern?

Wie auch bereits in der Kommentierung des DFKA e.V. zum Referentenentwurf der KassenSichV[7] dargestellt, ist ein Sicherheitsgewinn nicht erkennbar.

Umsetzung im INSIKA-Verfahren

Das INSIKA-Verfahren kann durch eine relativ einfache Erweiterung um eine interne Zeitquelle ergänzt werden.

Funktionsweise

Es wird zwischen zwei Modi für die Zeitquelle unterschieden:

- Externe Zeitquelle (Kompatibilitätsmodus – alle Funktionen identisch zur aktuellen Spezifikation)
- Interne Zeitquelle

Der neue Modus „interne Zeitquelle“ arbeitet wie folgt:

1. Der Modus wird bei der Personalisierung bestimmt, z. B. auf Basis eines festgelegten Umstellungstermins. Bei der Personalisierung wird das Sicherheitsmodul entsprechend der Bestellung für einen bestimmten Empfänger vorbereitet (u. a. werden die kryptografischen Schlüssel erzeugt).
2. Es gibt einen neuen Befehl, um die interne Zeit zu setzen:
   - Der Befehl liefert einen signierten Datensatz unter Vergabe einer Sequenznummer zur Aufzeichnung als Transaktion (damit ist jedes Setzen der Zeit dokumentiert).
   - Wurde der Befehl zum Setzen der Zeit nach einem Neustart der Sicherheitsein-

[5] Präsentation zum Fachgespräch „Schutz vor Manipulationen an digitalen Grundaufzeichnungen“ im BMF am 7. September 2017

[6] Quelle: http://static.rainfocus.com/oracle/oow17/sess/1493322921290001OicX/PF/CON4662%20JavaCard-20YearsofSecurityInnovationV1.1_1507095444215001OKJB.pdf, Seite 31

[7] https://www.dfka.net/wp-content/uploads/2017/04/DFKA-zur-KassenSichV-E-2017-04.pdf, Anlage, Abschnitt 3

richtung noch nicht ausgeführt (ist also keine interne Zeit vorhanden), können keine Transaktionen signiert werden – der Versuch führt zu einer Fehlermeldung.
- Durch die Nutzung sicherer Zeitstempel[8] in bestimmten Abständen, z. B. einmal am Tag, könnte die Qualität der Zeitinformation erhöht werden. Dazu müsste der Zeitstempel in die Signatur des Befehls zum Setzen der Zeit einbezogen und mit aufgezeichnet werden. Voraussetzung für den Bezug von sicheren Zeitstempeln wäre natürlich eine Internet-Verbindung.

3. Transaktionen werden nur unter Verwendung der internen Zeitquelle signiert. Die Zeit wird zusammen mit Signatur, Sequenznummer usw. zurückgeliefert. Sie muss in der Transaktion gespeichert und auf dem Beleg abgedruckt werden, um die Überprüfbarkeit der Daten sicherzustellen.

Praktische Umsetzung

Die Implementierung bedeutet eine relativ kleine Softwareerweiterung an bestehenden Implementierungen.

Sie erfordert jedoch eine Hardware für das Sicherheitsmodul mit geeigneten Funktionen zur Verwaltung der Zeitinformationen (siehe oben).

Kompatibilität

Im Modus „externe Zeitquelle“ wären neue INSIKA-Sicherheitsmodule kompatibel zu den momentan verfügbaren.

Um den Modus „interne Zeitquelle“ korrekt zu unterstützen, sind Erweiterungen an den Host-Systemen (Registrierkassen, Taxameter usw.) erforderlich. Systeme, die das Sicherheitsmodul zwischen den Transaktionen stromlos schalten, müssten so geändert werden, dass die Stromversorgung dauerhaft aktiv ist.

Um den Übergang zu erleichtern, könnte es erlaubt werden, für eine Übergangzeit weiterhin den Modus „externe Zeitquelle“ zu verwenden.

Fazit

- Durch eine interne Zeitquelle im Sicherheitsmodul kann ein bestimmter Angriff auf das System erschwert werden. Eine wesentliche Erhöhung der Sicherheit stellt dies jedoch nicht dar.
- Eine preiswerte Implementierung in einer Smartcard ist generell möglich – passende Karten sind allerdings derzeit noch nicht verfügbar.
- Das INSIKA-Verfahren kann durch eine einfache und geradlinige Erweiterung um eine interne Zeitquelle ergänzt werden.

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.

INSIKA wird seit 2012 in mehreren deutschen Städten erfolgreich als Sicherheitsmodul in vielen Tausend sogenannter Fiskal-Taxameter eingesetzt.

Das INSIKA-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.

Kontakt

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

www.insika.de
E-Mail: info@insika.de

[8] Ein Zeitstempel ist ein mit den Nutzdaten (dazu würde sinnvollerweise die Identifikation des Sicherheitsmoduls zusammen mit der aktuellen Sequenznummer genutzt) verbundener und digital signierter Datum/Uhrzeit-Wert. Stammt die Signatur von einem vertrauenswürdigen Absender, wird dadurch die Zeitinformation vertrauenswürdig.