INSIKA-Prüfverfahren für Kassenbelege und aufgezeichnete Daten

Jörg Wolff
Physikalisch-Technische Bundesanstalt (PTB)
Abbestraße 2-12, 10587 Berlin
joerg.wolff@ptb.de

Durch Prüfverfahren lässt sich die Integrität und Authentizität von INSIKA-Belegen und -Daten sicherstellen. Eine erfolgreiche Verifikation sichert somit die Zuordnung zum Urheber, die Vollständigkeit der jeweiligen Belege oder Daten und weist nach, dass diese nicht verändert wurden.

Der folgende Beitrag erläutert die Prüfverfahren aus einer technischen Betrachtungsweise. Zunächst wird das INSIKA-System im Überblick dargestellt. Danach werden die Inhalte von Kassenbelegen und aufzuzeichnenden Daten und die sich daraus ergebenen Möglichkeiten der Prüfung vorgestellt. Anschließend wird die durch INSIKA definierte Schnittstelle zum Datenexport dargelegt und abschließend die an der PTB entwickelte Prüfsoftware vorgestellt.

1 INSIKA-Systemüberblick

Bei Verwendung des INSIKA-Systems lassen sich mit elektronischen Registrierkassen und Taxametern aufgezeichnete Vorgänge sicher, schnell und automatisiert prüfen. Die dabei verwendeten Prüfverfahren lassen sich direkt aus dem System ableiten. In diesem Abschnitt soll daher zunächst ein Überblick zum INSIKA-System gegeben werden.

1.1 Nutzergruppen der Prüfverfahren

INSIKA-Prüfverfahren stehen grundsätzlich jedem zur Verfügung. Da die INSIKA-Spezifikationen auf Standards basieren und offen zugänglich sind, können Prüfwerkzeuge von verschiedenen Anbietern erstellt und genutzt werden. Die Nutzer der Prüfverfahren lassen sich in die folgenden Gruppen einteilen:

1.1.1 Unternehmer

Zunächst kann der Kassenbetreiber, also der Unternehmer selbst, jederzeit seine Daten in vollem Umfang einsehen und verifizieren. Somit ist eine Kontrolle von Daten vor einer Herausgabe an Dritte jederzeit problemlos möglich. Bei der Anwendung der Prüfverfahren hat der Urheber – hier also der Unternehmer – in allen Phasen die Rechte an den gesicherten Daten.

Durch die INSIKA-Prüfverfahren bietet sich dem Unternehmer zusätzlich die Möglichkeit, seine Kassen oder Taxameter auch im Innenverhältnis gegenüber den Bedienern abzusichern.

1.1.2 Muttergesellschaften, Dienstleister

Als zweite mögliche Anwender von Prüfverfahren lassen sich Muttergesellschaften oder externe Dienstleister benennen. Hierbei sind verschiedene Konstellationen denkbar, die im Wesentlichen vom Grad der Abhängigkeit der Unternehmen abhängen.

Auch Dienstleister aus den Bereichen IT, Archivierung, Steuerdaten o. ä. können im Auftrag des Unternehmers Prüfaufgaben übernehmen. So werden beispielsweise bei der Anwendung des INSIKA-Systems auf Taxameter die Daten aus dem Fahrzeug an einen Datendienstleister übergeben. Dieser kann im Auftrag des Unternehmers Prüfungen durchführen.

1.1.3 Finanzverwaltungen und Ordnungsbehörden

Finanzverwaltungen und Ordnungsbehörden bilden eine weitere Prüfinstanz. Bei korrekter Anwendung des Systems können diese im Rahmen einer Betriebsprüfung schnell auf gesicherte, herstellerunabhängige

PTB-Bericht IT-18
doi:10.7795/210.20130206a

und automatisiert auswertbare Informationen zurückgreifen.

Das System entspricht den in Deutschland geltenden „Grundsätzen zum Datenzugriff und der Prüfbarkeit digitaler Unterlagen“ [1] und ist konform zum Schreiben „Aufbewahrung digitaler Unterlagen bei Bargeschäften“ des Bundesfinanzministeriums vom November 2010 [2]. Durch die Absicherung von Umsätzen an Registrierkassen und Taxametern und einen einheitlichen Datenexport kann das System erheblich zur Vereinfachung, Beschleunigung und Objektivität von Betriebsprüfungen der Finanzverwaltungen beitragen.

In Branchen, die speziellen Regelungen unterliegen, können zusätzlich Aufsichtsbehörden ein Prüfinteresse besitzen. Ein Beispiel hierfür bilden im Bereich der Taxen die zuständigen Behörden für Konzessionen.

1.1.4 Hersteller von Registrierkassen oder Taxametern

Auch für die Hersteller von Registrierkassen oder Taxametern können sich Vorteile aus der Nutzung von INSIKA-Prüfverfahren ergeben. Zunächst kann jeder Hersteller Prüfverfahren implementieren und dem Kunden als Zusatznutzen anbieten. Bei klaren gesetzlichen Rahmenbedingungen ist es Herstellen von Registrierkassen zudem möglich, nachweisbar gesicherte Systeme anzubieten. Im Gegensatz zu anderen Systemen kann dabei auf den Aufwand und die Innovationsbeschränkung von Bauartzulassungen oder Zertifizierungen verzichtet werden.

Bei Taxametern bleibt die vorgeschriebene Bauartzulassung unverändert verpflichtend, da das INSIKA-System nur auf die Taxameter-Daten angewendet wird, das Gerät selbst aber nicht verändert.

1.2 INSIKA-Systemstruktur

Grundsätzlich ist die INSIKA-Systemstruktur für Registrierkassen und Taxametern durch die Schnittstellenspezifikationen festgelegt. Bei beiden Anwendungen werden Ursprungsdaten mit Hilfe digitaler Signaturen gesichert. Die Signaturen werden dabei durch eine Smartcard erzeugt. Diese Smartcard ist mit einer speziellen Software ausgestattet und wird bei INSIKA als „Tax Identification Module“ (TIM) bezeichnet. Abbildung 1 zeigt die grundlegende Systemstruktur am Beispiel von Registrierkassen.

Die TIM-Schnittstelle spezifiziert das Datenformat und die Kommunikation mit der Smartcard. Die signierten Daten werden in einem einheitlichen Format exportiert, diese Schnittstelle wird XML-

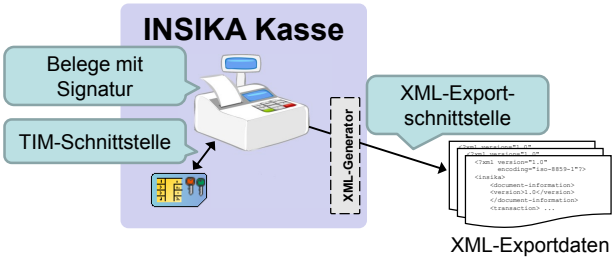


Abbildung 1: INSIKA-Schnittstellen

Exportschnittstelle genannt. Nachfolgend werden diese Schnittstellen detailliert betrachtet.

1.2.1 TIM-Schnittstelle

Über die TIM-Schnittstelle wird die Smartcard an das Kassensystem angebunden. Buchungsdaten werden über diese Schnittstelle von der Kasse an das TIM übergeben und zunächst durch dieses plausibilisiert. Bei positivem Ergebnis wird eine Signatur berechnet und in der Antwort zurückgegeben. Gleichzeitig werden dabei auf dem TIM die entsprechende Sequenznummer und die Summenspeicher aktualisiert. Durch einen sog. Tagesabschluss werden diese Summenspeicher vom TIM signiert ausgegeben.

Die TIM-Schnittstelle ist durch den Standard ISO/IEC 7816 Teil 1-4 in der physikalischen Schicht, sowie in der Sicherungs- und Anwendungsschicht definiert [3–6]. Die für INSIKA nötigen Erweiterungen auf Ebene der Anwendungsschicht sind in der „TIM-Schnittstellendokumentation“ spezifiziert [7, 8]. Das verwendete ECDSA-Signaturverfahren ist z. B. in FIPS186 des NIST definiert [9].

1.2.2 XML-Exportschnittstelle

Um alle Buchungen und Tagesabschlüsse mit den entsprechenden Signaturen abzuspeichern, muss eine INSIKA-Kasse ein Journal führen. Für die Datenspeicherung in diesem Journal bestehen seitens des INSIKA-Systems keine Vorgaben, sie ist also dem Kassenhersteller überlassen. Einzig die Exportdaten müssen aus dem Journal generierbar sein, d. h. die Buchungen und Tagesabschlüsse müssen sich inklusive ihrer Signaturen vollständig zurückgewinnen lassen.

Als Datenformat wird die Auszeichnungssprache XML („Extensible Markup Language“) verwendet. Das Kassensystem selbst muss dabei nicht unbedingt XML-Dateien generieren können. Für diese Aufgabe ist auch ein nachgeschaltetes System in Form eines PC o. ä. nutzbar. In der Abbildung 1 wird dies durch die optional gekennzeichnete Einheit „XML-Generator“

deutlich gemacht. Die XML-Exportschnittstelle ist eine Schnittstelle zum einseitigen Datenexport, deren Struktur und Form durch ein INSIKA-XML-Schema definiert ist [10].

1.2.3 Gedruckte Belege

In Abbildung 1 ist zu erkennen, dass bei Registrierkassen grundsätzlich gedruckte Belege mit Signatur ausgegeben werden. Hauptzweck dieser Belege ist der unmittelbare Nachweis der Signaturerstellung.

1.2.4 Webservice für Taxameterdaten

Auf Grund der besonderen Verhältnisse bei Taxametern und angeschlossenen Quittungsdruckern wurde hierfür eine erweiterte Systemstruktur entworfen. Dabei werden die Daten permanent aus dem Fahrzeug mit Hilfe eines RESTful-Webservice auf einen Server übertragen. Details dieser zusätzlichen Schnittstelle finden sich in der zugehörigen Spezifikation [11].

Die TIM-Schnittstelle und die XML-Exportschnittstelle sind jedoch die selben wie bei Registrierkassen. Damit sind auch die INSIKA-Prüfverfahren für Daten in beiden Anwendungen identisch.

1.3 Prüfbare Daten

Grundsätzlich können im INSIKA-System drei verschiedene Daten zur Prüfung herangezogen werden: XML-Exportdaten, gedruckte Belege und TIM-Daten. Die Prüfung von bereitgestellten XML-Exportdaten stellt den Normalfall dar. Die stichprobenhafte Prüfung von Belegen und die Zuordnung von Belegen zu Exportdaten sollte diese Prüfung untermauern. Das Auswerten der TIM-Daten ist nur als Rückfall gedacht, sofern XML-Exportdaten nicht mehr vorhanden sein sollten.

1.4 Signierte Buchungsdaten

Wie zuvor beschrieben, werden auf dem TIM die Buchungsdaten vor der Signaturberechnung plausibilisiert. Bei positivem Ergebnis sind die Buchungsdaten in Bezug auf Umsatz, Umsatzsteuersatz und Umsatzsteuer rechnerisch richtig. Der Buchungsdatensatz wird durch das TIM signiert und die Signatur wird an die Kasse zurückgegeben. Bei negativem Ergebnis der Plausibilisierung wird vom TIM anstelle der Signatur ein Fehlercode zurückgeben.

In der späteren Betrachtung lassen sich grundsätzlich nur Datenelemente verifizieren, über die die Signatur direkt oder indirekt gebildet wurde. Alle möglicherweise darüber hinaus bereitgestellten Daten haben aus INSIKA-Sicht rein informativen Charakter. Im Rahmen einer Buchung gehen die folgenden Datenelemente in die Signatur ein:

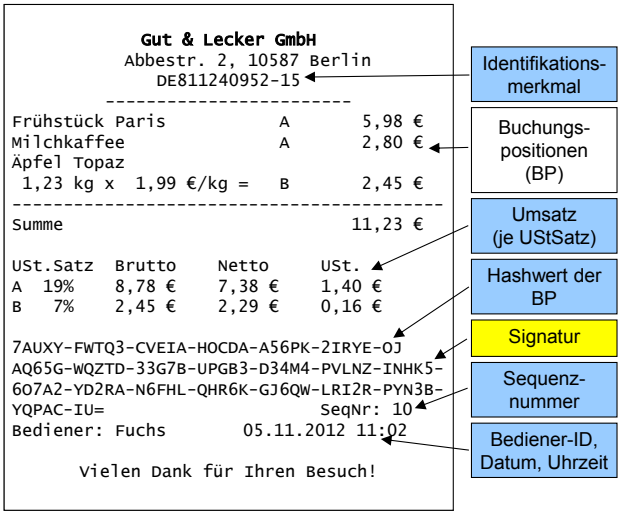


Abbildung 2: INSIKA-Kassenbeleg mit signierten Datenelementen

- Identifikationsmerkmal,
- Umsatz je Umsatzsteuersatz,
- Hashwert der Buchungspositionen,
- Sequenznummer,
- Bediener-Identifikation,
- Datum und
- Uhrzeit.

Diese signierten Datenelemente lassen sich sowohl in den XML-Exportdaten als auch auf dem Beleg wiederfinden. Die Abbildung 2 zeigt dazu beispielhaft einen INSIKA-Beleg. Die signierten Datenelemente sind hierbei blau markiert und werden nun nachfolgend näher erläutert.

1.4.1 Identifikationsmerkmal

Das Identifikationsmerkmal dient der eindeutigen Zuordnung des TIM in Bezug auf die Umsatzsteuer [12]. Da diese Steuer durch Unternehmen abgeführt wird, eignet sich in Deutschland die Wirtschafts-Identifikationsnummer (W-IdNr) als Identifikation. Die W-IdNr ist das Gegenstück zur persönlichen Steuer-Identifikationsnummer und wird wie diese nur einmal vergeben [13].

Bis zur Einführung der W-IdNr kann auch die Umsatzsteuer-Identifikationsnummer (USt-IdNr) verwendet werden. Diese Nummer wird in der gesamten Europäischen Union an Unternehmen eindeutig vergeben. Um die einzelnen TIMs eines Unternehmens direkt identifizieren zu können, wird die W-IdNr bzw.

USt-IdNr um einen Bindestrich und eine forlaufende Zahl erweitert. Alles zusammen bildet dann das Identifikationsmerkmal.

Durch die fortlaufende Zahl kann die Anzahl der TIMs je Unternehmen jederzeit leicht nachvollzogen werden. Dies ist eine wichtige Voraussetzung in der korrekten Anwendung des INSIKA-Systems.

1.4.2 Umsatz je Umsatzsteuersatz

Der Umsatz einer Buchung wird immer aufgeschlüsselt für jeden Umsatzsteuersatz signiert. In einem Buchungsdatensatz können gleichzeitig Umsatzsteueranteile von sechs verschiedenen Umsatzsteuersätzen an das TIM übergeben werden. Im Abschnitt 4.1 wird dies noch näher erläutert.

1.4.3 Hashwert der Buchungspositionen

Vor der Übergabe der Buchungsdaten an das TIM wird über die Buchungspositionen ein Hashwert – also eine Art eindeutiger Fingerabdruck – berechnet. Mit „Hashwert“ wird bei INSIKA ausschließlich das Ergebnis einer kryptografisch sicheren Hashfunktion bezeichnet. Aufgrund der kurzen Ergebnislänge wird in der derzeitigen Spezifikation das SHA-1 Verfahren genutzt [14]. Prinzipiell lassen sich aber auch andere Hashfunktionen festlegen.

Um diesen Hashwert zu berechnen, werden die Buchungspositionen nach einer definierten Vorschrift abgebildet. Da in verschiedenen Einsatzgebieten des Systems unterschiedliche Datenobjekte abgebildet werden müssen, wurden sogenannte „INSIKA-Profile“ definiert. Diese Profile werden nachfolgend im Abschnitt 1.5 erläutert.

Der Hashwert der Buchungspositionen geht direkt in die Signatur ein. Jede nachträgliche Veränderung der Buchungspositionen würde zu einem veränderten Hashwert führen und damit eindeutig erkannt werden.

1.4.4 Sequenznummer

Auch die Sequenznummer ist Teil des signierten Buchungsdatensatzes. Im INSIKA-System wird die Sequenznummer durch das TIM vergeben und fortlaufend mit jeder Signatur inkrementiert. Da die Sequenznummer auf dem TIM gespeichert wird, besitzt diese Nummer einen hohen Grad an Manipulationssicherheit. Die Sequenznummer bildet eine unabhängige Basis, aus der sich die Chronologie von Buchungen und Tagesabschlüssen wiederherstellen lässt.

1.4.5 Bediener-Identifikation, Datum und Uhrzeit

Die Bediener-Identifikation, Datum und Uhrzeit gehen ebenfalls mit in die Signatur ein. Wie nachfolgend noch im Abschnitt 3.5 erläutert wird, werden diese Daten jedoch nur als Zusatzinformationen behandelt und nicht zur Prüfung der Konsistenz oder zur Wiederherstellung der Chronologie genutzt.

1.5 INSIKA-Profile

INSIKA-Profile dienen der Abbildung anwendungsspezifischer Daten eines Systems. Zur Zeit sind Profile für Registrierkassen und für Taxameter spezifiziert.

Ein Profil definiert die Datenobjekte, über die der Hashwert der Buchungspositionen gebildet wird. Wie zuvor im Abschnitt 1.4.3 beschrieben, wird im Rahmen einer Buchung dieser Hashwert zusammen mit den anderen zu signierenden Datenobjekten an das TIM übergeben und dort signiert.

Die Datenobjekte eines Profils, also die Buchungspositionen selbst, werden nicht an das TIM übergeben. Da jedoch der Hashwert dieser Datenobjekte signiert wird, gehen auch diese Datenobjekte indirekt in die Signatur mit ein. Somit können eine große Zahl von Datenobjekten in die Signatur eingehen, ohne dass diese auf der TIM-Schnittstelle übertragen werden müssen. Die Zeit der Datenübertragung und Signaturerstellung ist damit unabhängig von der Anzahl dieser Datenobjekte.

Durch das Konzept der Profile ist es zudem möglich, das INSIKA-System auf unterschiedliche Anwendungen anzupassen. Insbesondere lassen sich hiermit verschiedene messwertverarbeitende Systeme abbilden. Dabei finden sich eine Reihe von Analogien zur Sicherung von Messdaten in verteilten Messsystemen [15]. Bei allen Anpassungen durch Profile kann das Sicherungselement, also das TIM, unverändert bleiben.

1.5.1 Profil Registrierkasse

Dieses Profil ist für die gesamte Bandbreite der Registrierkassen von embedded Plattformen, PC-basierten Point-of-Sale (POS) Systemen bis zu verteilten Kassensystemen nutzbar. Es definiert für jede Buchungsposition die folgenden Datenobjekte:

- Menge/Anzahl,
- Mengeneinheit,
- handelsübliche Bezeichnung,
- Merker (Rabatt, Aufschlag, Gutschein,..),
- Preis je Umsatzsteuersatz

Damit werden auch gemessene Größen aus verbundenen Messgeräten definiert abgebildet. Nach der Zusammenstellung der Buchungspositionen wird über diesen Datensatz dann der Hashwert der Buchungspositionen berechnet. Dies kann in der Kasse oder auch auf dem TIM selbst durchgeführt werden. Weitere Details finden sich in der Spezifikation dieses Profils [7].

1.5.2 Profil Taxameter

Mit dem Profil für Taxameter wurde das INSIKA-System für Taxameterdaten erweitert. Dieses Profil kann für alle Taxameter verwendet werden, deren Bauart nach der Europäischen Messgeräterichtline 2004/22/EG („MID“) geprüft und zugelassen ist [16]. Die Zulassung des Taxameters wird dabei in keiner Weise berührt.

Die Datenobjekte diese Profils basieren auf den in der MID definierten Informationen. Eine Fahrt wird durch eine Buchung abgebildet, die die Datenobjekte aus 1.4 und die folgenden enthält:

- zurückgelegte Strecke,
- Gesamtsumme einer Fahrt je Umsatzsteuersatz,
- Datum Fahrtbeginn,
- Uhrzeit Fahrtbeginn

Auch Schichten (also die An- und Abmeldung des Fahrers am Taxameter) werden abgebildet, sofern das Taxameter dazu in der Lage ist. Detaillierte Informationen finden sich in der Spezifikation des Profils für Taxameter [17].

1.6 Zertifikatsverwaltung

Die INSIKA-Prüfverfahren sind fest in das INSIKA-Gesamtsystem eingebettet. Zum besseren Verständnis soll hier zunächst ein kurzer Überblick zur Zertifikatsverwaltung, der sog. Public-Key Infrastructure (PKI), gegeben werden. Die vereinfachten Instanzen und Abläufe der Zertifikatsverwaltung zeigt die Abbildung 3.

Da das INSIKA-System auf asymmetrischer Kryptographie beruht, lassen sich auch hier mit einem privaten Schlüssel signierte Daten durch den dazugehörigen öffentlichen Schlüssel verifizieren. Das Paar aus privatem und öffentlichem Schlüssel wird vor der Ausgabe des TIM auf diesem generiert. Der private Schlüssel ist dabei nicht lesbar und verlässt das TIM niemals. Der öffentliche Schlüssel wird vor der Ausgabe des TIM ausgelesen und zusammen mit dem Identifikationsmerkmal des Unternehmers in einem Zertifikat abgelegt. In der Abbildung 3 sind schematisch der private und der öffentliche Schlüssel rot bzw. grün eingezeichnet.

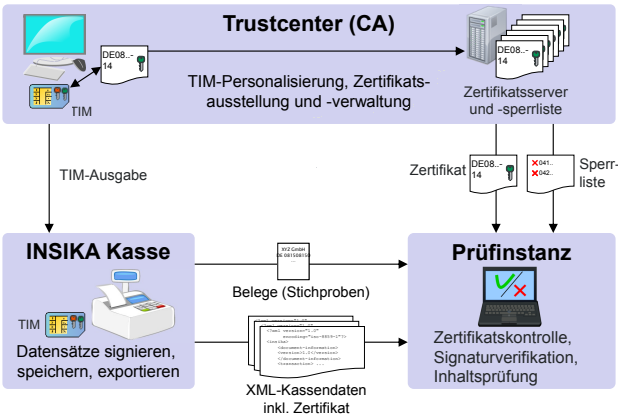


Abbildung 3: Zertifikatsverwaltung (vereinfacht)

Die zuvor genannten Schritte vor der Ausgabe des TIM dienen also der Zuordnung des TIM auf den Unternehmer. Diese sog. Personalisierung wird durch eine zentrale Stelle oder ein privat betriebenes Trustcenter durchgeführt.

Durch das Zertifikat wird die Authentizität, also die eindeutige Zuordnung des TIM und der damit signierten Daten und Belege zu einem Unternehmer, hergestellt. Das Zertifikat findet sich sowohl auf dem TIM als auch auf dem Zertifikatsserver. Die Gültigkeit kann anhand eines Abgleichs mit der Sperrliste („Certificate Revocation List“) überprüft werden. Bei Verlust des TIM, Auflösung des Unternehmens o. ä. kann der Unternehmer das zugehörige Zertifikat auf die Sperrliste setzen lassen. Ab diesem Zeitpunkt können dann keine gültigen Signaturen mehr erzeugt werden. Die Sperrliste und der Zertifikatsserver werden durch die zentrale Stelle bzw. das Trustcenter bereitgehalten und gepflegt.

2 Prüfverfahren für Belege

Die Prüfung gedruckter Kassenbelege kann in zwei unterschiedlichen Tiefen erfolgen. Der übliche Fall ist die Verifikation der Signatur. Dazu werden die unter 1.4 erläuterten signierten Buchungsdaten, die Signatur und der öffentliche Schlüssel benötigt. Durch die Verifikation des Hashwerts der Buchungspositionen lässt sich die Prüfung zusätzlich auf die einzelnen Buchungspositionen ausweiten. Diese Option wird am Ende dieses Abschnitts erläutert.

2.1 Verifikation der Signatur

Wie bereits in der Abbildung 2 dargestellt, können alle signierten Buchungsdaten dem gedruckten Beleg entnommen werden. Bei der Belegverifikation

werden diese Buchungsdaten wieder auf das Format der TIM-Schnittstelle zurückgeführt. Damit wird genau der Datensatz erstellt, der ursprünglich durch das TIM signiert wurde. Zusammen mit der ebenfalls auf dem Beleg gedruckten Signatur und dem öffentlichen Schlüssel des TIM kann dann die Verifikation durchgeführt werden.

Da der öffentliche Schlüssel nicht auf dem Beleg gedruckt wird, muss dieser aus dem Zertifikat gewonnen werden. Anhand des auf dem Beleg gedruckten Identifikationsmerkmals kann auf dem Zertifikatsserver das jeweilige Zertifikat – und damit auch der öffentliche Schlüssel – gefunden werden. Wie in Abbildung 3 gezeigt, kann jede Prüfinstanz auf diesen Zertifikatsserver zugreifen. Die Prüfinstanz kann aber auch lokale Kopien vorhalten, da Zertifikate nur eine geringe Speichergröße besitzen. Die Belegverifikation lässt sich beispielsweise mit der nachfolgend im Abschnitt 5 erläuterten IVM-Software durchführen.

2.2 Zeichenersetzung der Buchungspositionen

Abgesehen von der Bedingung, dass sich ein gedruckter Beleg verifizieren lassen muss, werden durch das INSIKA-System keine Vorgaben in Bezug auf Format, Größe oder Schriftart des Belegs gemacht. Um bei der Zurückgewinnung von gedruckten Texten dennoch robuste Ergebnisse zu erhalten, werden Textfelder vor der Hashwertbildung (und somit vor dem Signieren und vor dem Drucken) einer Zeichenersetzung unterzogen. Hierbei werden besonders fehleranfällige Zeichen und Sonderzeichen weggelassen oder durch ein festgelegtes Zeichen ersetzt [7].

So werden beispielsweise Leerzeichen ausgelassen, da sie sich nicht eindeutig aus gedruckten Belegen zurückgewinnen lassen. Auch Umlaute werden aufgrund ihrer unterschiedlichen Repräsentation in den jeweiligen Zeichensätzen durch ein definiertes Zeichen ersetzt. Diese Zeichenersetzung findet intern als Vorstufe der Hashwertbildung statt und ändert am Ausdruck des Belegs selbstverständlich nichts.

2.3 Format von Hashwert der Buchungspositionen und Signatur

2.3.1 Base32-Kodierung

Der Hashwert der Buchungspositionen und die Signatur müssen auf jedem INSIKA-Beleg gedruckt werden. Um den dazu nötigen Platz auf dem Beleg zu minimieren, wurde in Abbildung 2 eine Base32-Kodierung genutzt [18]. Damit verkürzt sich die Ausdrucklänge gegenüber einem Ausdruck in hexadezimaler Kodierung um ca. ein Fünftel auf 32 bzw. 77 Zeichen. Eine Kodierung in Base64 würde die Ausdrucklänge weiter reduzieren, allerdings sind die dabei verwendeten Groß- und Kleinbuchstaben sehr fehleranfällig in der Erfassung.

Die Base32-Kodierung erlaubt ein gutes Verhältnis zwischen der Ausdrucklänge und der Fehlerrate bei der Rückgewinnung der Daten aus dem gedruckten Beleg. In der Prüfung kann diese Kodierung jederzeit per Bilderkennung, Stift-Scanner oder auch manuell eingelesen werden.

Da jeder alphanumerische Drucker in der Lage ist, die Base32-Kodierung auszugeben, bildet dies eine einfache Möglichkeit zur Integration von INSIKA in bestehende Kassensysteme.

2.3.2 QR-Code

In der Prüfung ergeben sich weitere Vereinfachungen durch die Verwendung von grafischen Codes. Insbesondere bieten sich dafür standardisierte 2D-Codes wie PDF417, Data Matrix oder QR-Code an [19]. Bei Verwendung dieser Codes lassen sich zudem bereits integrierte, leistungsfähige Verfahren zur Fehlererkennung und -korrektur nutzen.

Abbildung 4 zeigt beispielhaft einen Kassenbeleg mit QR-Code. In diesem Code sind die signierten Buchungsdaten und die Signatur enthalten.

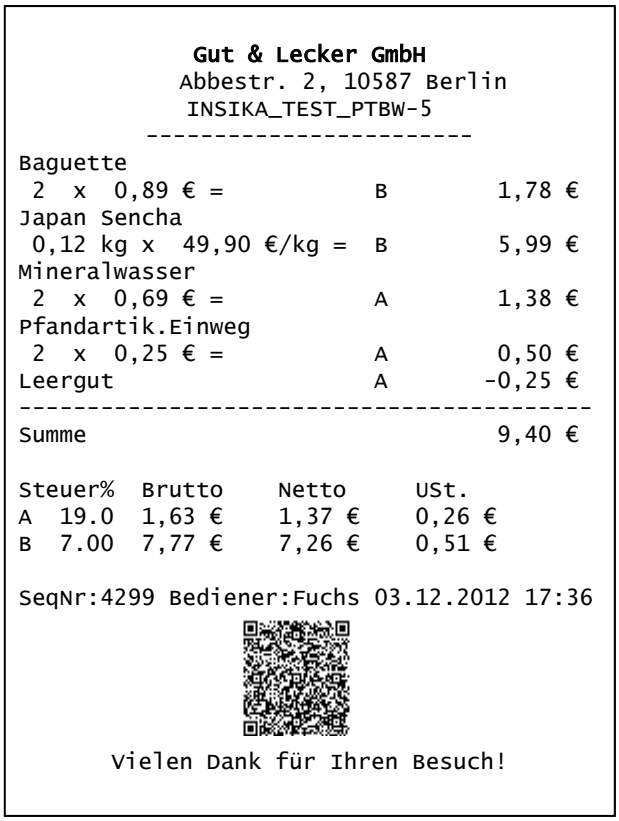
Da viele Drucker bereits heute QR-Codes generieren und drucken können, ist die Integration dieser Technik in Kassensysteme in vielen Fällen einfach und kostengünstig.

2.4 Online-Verifikation

Um die Belegprüfung noch weiter zu vereinfachen, sind die Daten des QR-Code in Form einer URL (Uniform Resource Locator) eingebettet. Diese URL[1] kann mit jedem Lesegerät für QR-Codes gelesen und aufgerufen werden. Eine spezielle Software auf dem Lesegerät ist dafür nicht notwendig.

Zur Prüfung wird einfach der QR-Code gescannt und die enthaltene URL aufgerufen. Beim Aufruf werden die signierten Buchungsdaten und die Signatur an einen Verifikationsservice auf dem angegebenen Server übergeben. Auf diesem Server wird mit Hilfe des

[1] Inhalt des QR-Code aus Abbildung 4: `http://insika.de/verify.php?t1=zQQgEhIDzgIXNsYFZnVjaHPHFMDqz775LBLNQF1nA4ak0O_gIfdM4QjYAhY82wIZAOII2AJ3fNsCBwDEEE1OU01LQV9URVNUX1BUQ1fFAQXLAhDLnjBcFrO4v0fzbkRNp-WI8vobRWB9KBMMoHbhhbX5I3XH9u85B_azU7LmA7ZMr-ixSHg=`



Gut & Lecker GmbH
Abbestr. 2, 10587 Berlin
INSIKA_TEST_PTBW-5

Baguette
2 x 0,89 € = B 1,78 €
Japan Sencha
0,12 kg x 49,90 €/kg = B 5,99 €
Mineralwasser
2 x 0,69 € = A 1,38 €
Pfandartik.Einweg
2 x 0,25 € = A 0,50 €
Leergut A -0,25 €

Summe 9,40 €

Steuer%	Brutto	Netto	USt.
A 19.0	1,63 €	1,37 €	0,26 €
B 7.00	7,77 €	7,26 €	0,51 €

SeqNr:4299 Bediener:Fuchs 03.12.2012 17:36

Vielen Dank für Ihren Besuch!

Abbildung 4: INSIKA-Kassenbeleg mit QR-Code

Identifikationsmerkmals das Zertifikat vom Zertifikatsserver abgefragt und ein Abgleich mit der aktuellen Sperrliste durchgeführt. Danach wird der öffentliche Schlüssel aus dem Zertifikat ausgelesen. Zusammen mit den signierten Buchungsdaten wird dann auf dem Server die Signatur verifiziert und das Ergebnis auf einer Webseite dargestellt.

Abbildung 5 zeigt das Ergebnis für die erfolgreiche Online-Verfikation des Belegs aus Abbildung 4. Deutlich zu erkennen ist dabei die Übereinstimmung der signierten Inhalte (Sequenznummer, Umsatz, usw) in beiden Abbildungen.

Mittlerweile können eine Vielzahl von Mobiltelefonen, Smartphones oder Handscannern QR-Codes lesen. Sofern diese Geräte einen Zugang zum Internet besitzen, können sie für eine sofortige Belegprüfung genutzt werden. Durch diese Online-Verfikation ist es für jeden Kunden möglich, den Beleg zu prüfen.

Denkbar wäre, dieses Potential mit Hilfe von Anreizsystemen zu nutzen und damit eine sehr hohe Prüfdichte zu erreichen. So könnten Vorgaben zur Anerkennung von Belegen seitens der Finanzverwaltung Anreize schaffen. Auch wäre die Verknüpfung der Online-Verifikation mit Verlosungen vorstellbar.

Sofern gesellschaftlich akzeptiert und datenschutzrechtlich unbedenklich, könnte die Online-Verifikation

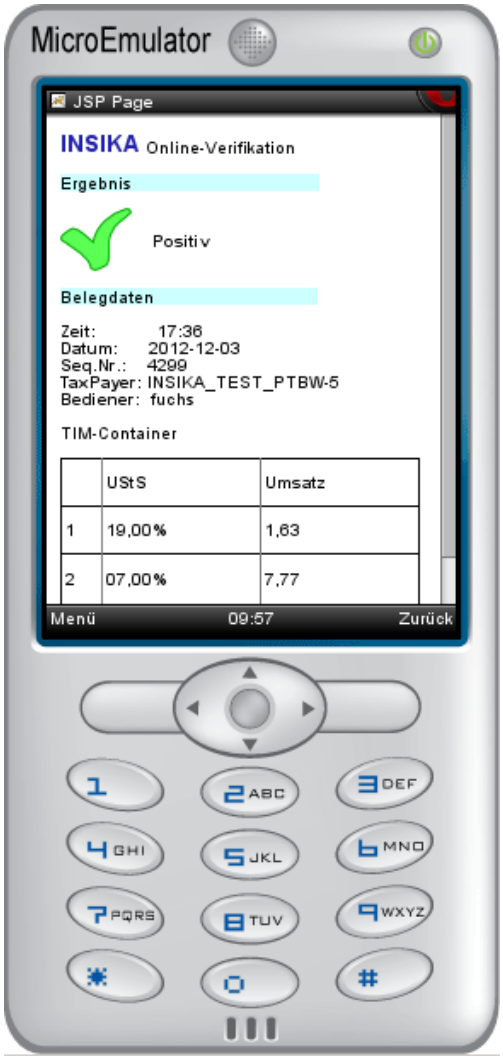


Abbildung 5: Ergebnis der Online-Verifikation des Belegs aus Abbildung 4

auch zur Sammlung von Stichproben zur späteren Prüfung mit eingereichten Daten genutzt werden. Nicht nur aus diesem Grund sollte der Service der Online-Verifikation durch eine vertrauenswürdige Instanz und zukünftig auf einem gesicherten Weg bereitgestellt werden.

2.5 Verifikation des Hashwerts der Buchungspositionen

Die Prüftiefe in der Belegprüfung kann weiter erhöht werden, in dem auch die Richtigkeit der auf dem Beleg gedruckten Buchungspositionen kontrolliert wird. Die Buchungspositionen werden durch den gedruckten und signierten Hashwert eindeutig abgebildet. Anhand der gedruckten Buchungspositionen kann nun dieser Hashwert neu berechnet und mit dem gedruckten verglichen werden. Hierzu sind die gleichen Schritte wie bei der Erstellung dieses Hashwerts vor dem Signie-

ren nötig. Bei der Prüfung werden somit zuerst die Buchungspositionen aus dem Beleg erfasst und in einer fest definierten Weise abgebildet. Anschließend werden die Textfelder durch die Zeichenersetzung gewandelt. Stimmt der nun über die Buchungspositionen ermitteltet Hashwert mit dem gedruckten Hashwert überein, sind auch die gedruckten Buchungspositionen korrekt.

3 Prüfverfahren für XML-Exportdaten

Die Prüfung von XML-Exportdaten – also quasi dem Kassenjournal – stellt den üblichen Fall der Prüfung dar. Auf Anfrage der Prüfinstanz stellt der Unternehmer XML-Exportdaten über einen bestimmten Zeitraum bereit. Die Prüfung läuft nun in drei Stufen ab. Auf die Validierung des XML-Formats folgt die Verfikation der Signaturen, worauf schließlich die Prüfung der Inhalte aufsetzt. Diese Prüfschritte und das XML-Format werden nachfolgend genauer erläutert.

3.1 XML zum Datenexport

Die Extensible Markup Language (XML) ist eine Beschreibungssprache, die durch das World-Wide-Web Consortium (W3C) standardisiert wurde [20]. XML wird vor allem zum Datenaustausch zwischen maschinellen Systemen eingesetzt. Im INSIKA-System kann durch die Verwendung von XML der Datenexport einheitlich und herstellerunabhängig definiert werden. Damit erleichtert sich eine Prüfung erheblich. Zudem ist diese Prüfung unabhängig von Ort, Plattform und Medium. Bei der Datenübermittlung können Internet-Protokolle (HTTPS, E-Mail, usw.) oder beliebige Datenträger (USB-Sticks, CD-ROMs, Speicherkarten, usw.) zum Einsatz kommen. Sofern nötig, können XML-Daten meist zu einem hohen Grad komprimiert werden.

Auch eine Wandlung des INSIKA XML-Exportformats entsprechend anderer Vorschriften ist einfach möglich. So wird XML auch im „Standard Audit File – Tax“ (SAF-T) der OECD verwendet. Kassendaten können einen Bestandteil des SAF-T bilden, allerdings werden dabei keine Signaturen verwendet. Daher ist die Verwendung von SAF-T in dieser Form hier zur Zeit nicht zielführend.

3.2 Formate der XML-Exportdaten

XML-Dokumente enthalten ausschließlich Textzeichen und lassen sich daher mit jedem Editor oder Webbrowser darstellen. Die INSIKA-XML-Exportdaten enthalten Zertifikate, Buchungen und Tagesabschlüsse. Es sind zwei Formate definiert, die nachfolgend als „Klartext“ und „Base64“ bezeichnet werden.

In der INSIKA-XML-Variante „Klartext“ sind die Daten in lesbarer Form abgelegt. In der Abbildung 6 ist eine solche XML-Exportdatei beispielhaft für eine Buchung dargestellt. Wie im XML üblich, werden die Informationen als Textzeichen kodiert und zwischen öffnenden und schließenden Bezeichnern („Tags“) abgelegt. Die Tags sind an den Zeichen ,,<..>‘‘ und ,,</..>‘‘ zu erkennen und für INSIKA eindeutig definiert. Die Abbildung hierarchischer Ordnungen wird dabei durch Verschachtelung vorgenommen. XML ist hierfür besser geeignet als tabellenorientierte Formate.

Abbildung 4 und 6 zeigen den Beleg und die XML-Daten ein und derselben Buchung. Beim Vergleich ist deutlich zu erkennen, dass alle signaturrelevanten Datenelemente und Buchungspositionen des Belegs auch in der XML-Datei wiederzufinden sind. Beispielhaft sei auf den Umsatz von 7,77 € zum reduzierten Umsatzsteuersatz in Abbildung 4 und den zugehörigen Umsatz in Cent `<turnover>777</turnover>` in Abbildung 6 hingewiesen. Auch die Sequenznummer 4299 findet sich auf dem Beleg und in den zugehörigen Daten.

Die zweite INSIKA-XML-Variante „Base64“ wurde geschaffen, um eine sehr einfache Implementierung des Systems zu ermöglichen. In der Kasse werden dazu die binären Telegramme der TIM-Schnittstelle in beliebiger Form abgelegt. Zum Datenexport werden diese Telegramme in die textbasierte Base64-Kodierung [18] gewandelt und in eine einfache XML-Struktur abgelegt. Diese Lösung eignet sich insbesondere für Kassensysteme die bisher kein Journal führten, stark ressourcenbegrenzte Systeme und für Taxameter.

3.3 Validierung von XML-Dokumenten

Die erste Stufe der Prüfung von XML-Dokumenten ist die Validierung, d. h. die Prüfung auf Struktur und Format. Da die XML-Dokumente von maschinellen Systemen generiert werden, sind Fehler hierbei vorrangig in der Phase der Systemimplementierung oder bei beschädigten Dokumenten zu erwarten.

Zur Validierung wird ein XML-Schema genutzt, dass alle INSIKA-spezifischen XML-Tags, Datentypen und die dazugehörigen Strukturen festlegt [10, 21]. Durch die Validierung kann automatisch die korrekte Bedienung der XML-Exportschnittstelle sichergestellt werden.

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<insika xmlns="http://insika.de/export" xmlns:xsi="
    http://www.w3.org/2001/XMLSchema-instance" xsi:
    schemaLocation="http://insika.de/export
    INSIKA_ExportT106-04.xsd">
  <document-information>
    <version>1.0</version>
  </document-information>
  <timParams>
    <timVersion>T.1.1.0</timVersion>
    <tpId>INSIKA_TEST_PTBW</tpId>
    <tpIdNo>5</tpIdNo>
    <itemProfile>1</itemProfile>
    <certificate>MIIC/D ... udlfcWGYyLEdE/Q0Ke
    </certificate>
  </timParams>
  <transaction>
    <date>20121203</date>
    <time>1736</time>
    <operatorId>Fuchs</operatorId>
    <itemList profile="cashRegister">
      <item>
        <qnt>2</qnt>
        <name>Baguette</name>
        <price2>178</price2>
      </item>
      <item>
        <qnt>0.12</qnt>
        <unit>kg</unit>
        <name>Japan Sencha</name>
        <price2>599</price2>
      </item>
      <item>
        <qnt>2</qnt>
        <name>Mineralwasser</name>
        <price1>138</price1>
      </item>
      <item>
        <qnt>2</qnt>
        <name>Pfandartik.Einweg</name>
        <price1>50</price1>
      </item>
      <item>
        <qnt>1</qnt>
        <name>Leergut</name>
        <price1>-25</price1>
      </item>
    </itemList>
    <hashTransactionItems>
    C0EACFBEF92C12CD405D670386A4D0EFE021F74C
    </hashTransactionItems>
    <currency>0978</currency>
    <containerVat1>
      <turnover>163</turnover>
      <turnoverNeg>25</turnoverNeg>
      <vat>26</vat>
      <vatRate>1900</vatRate>
    </containerVat1>
    <containerVat2>
      <turnover>777</turnover>
      <vat>51</vat>
      <vatRate>0700</vatRate>
    </containerVat2>
    <tpId>INSIKA_TEST_PTBW</tpId>
    <tpIdNo>5</tpIdNo>
    <seqNoTransaction>4299</seqNoTransaction>
    <sig>5C16B3B8BF47F36E444DA7E588F2FA1B4560
    7D28130CA076E185B5F92375C7F6EF3907F6B353B
    2E603B64CAFE8B14878</sig>
  </transaction>
</insika>
```

Abbildung 6: „Klartext“-XML-Exportdatei mit der Buchung aus Abbildung 4

3.4 Verifikation der Signaturen

Die Verifikation der Signaturen bildet die nachfolgende Prüfstufe. Bei positivem Ergebnis werden die durch die Signatur gesicherten Daten in Integrität und Authentizität bestätigt. Wie bereits im Abschnitt 1.4 erwähnt, gilt dies nur für die signierten Datenelemente.

Die im Abschnitt 5 nachfolgend beschriebene IVM-Software führt diese Signaturverifikation automatisiert durch. Intern werden dazu die im XML-Dokument enthaltenen Textdaten wieder in das Format auf der TIM-Schnittstelle gewandelt. Zusammen mit den durch das TIM ergänzten Informationen ergibt sich dann der Datensatz, der im TIM signiert wurde. Die Verifikation kann aus diesem Datensatz, dem öffentlichen Schlüssel und der Signatur vorgenommen werden. Im Ergebnis wird die Signatur bestätigt oder als fehlerhaft gekennzeichnet. Durch die Signaturverifikation kann in folgenden Prüfstufen auf vertrauenswürdige Daten zurückgegriffen werden.

3.5 Konsistenz von Exportdaten

Im vorhergehenden Abschnitt wurde gezeigt, wie sich in der Prüfung die Integrität und Authentizität von Exportdaten nachweisen lässt. Aufgrund des Systemkonzepts kann zudem die Konsistenz der erfassten Daten geprüft werden.

Um die Zuverlässigkeit des Systems zu erhöhen, wird die Chronologie von Buchungen und Tagesabschlüssen grundsätzlich nicht durch Datum und Uhrzeit sichergestellt. Wie bereits beschrieben, werden zur chronologischen Ordnung die vom TIM vergebenen Sequenznummern genutzt. Diese sind nicht rücksetzbar und werden mit jeder Signaturvergabe inkrementiert. Dadurch lässt sich die korrekte Reihenfolge von Buchungen und Tagesabschlüssen wiederherstellen. Auch eventuell vorhandene Lücken in den Exportdaten (wie fehlende Buchungen oder Tagesabschlüsse) oder doppelte Datensätze (z. B. durch Bedienungsfehler) sind damit automatisiert auffindbar.

Im INSIKA-System wird eine unbestimmte Anzahl von Buchungen immer durch einen Tagesabschluss abgeschlossen. Der Umsatz zwischen zwei Tagesabschlüssen muss somit auch den Umsatzsummen der eingeschlossenen Buchungen entsprechen. Für die Prüfung heißt das, dass die Signaturverifikation von einzelnen Buchungen unter Einschränkungen entfallen kann. Somit würden nur die Signaturen der Tagesabschlüsse und die Übereinstimmung mit den eingeschlossenen Umsätzen der Buchungen überprüft. Einzig Umsatzverschiebungen zwischen Buchungen ließen sich damit nicht erkennen. Diese Vereinfachung

bietet die Möglichkeit, die Prüfung noch weiter zu beschleunigen.

3.6 Stichproben in Exportdaten

Die grundlegende Voraussetzung für das INSIKA-System ist der zeitnahe Nachweis der Signaturerstellung durch das TIM. Üblicherweise wird dies durch die verpflichtende Ausgabe eines signierten Belegs erfüllt. Jeder Beleg muss sich wiederum in den entsprechenden Exportdaten wiederfinden lassen. Vorhandene Belege können somit nicht nur in ihrer Gültigkeit geprüft werden, sondern bilden auch die Grundlage für Stichproben in den XML-Exportdaten. Anhand dieser Stichproben kann die korrekte und durchgängige Verwendung des TIM überprüft werden. Der Grad ausreichender Sicherheit ist dabei auf der Basis von statistischen Methoden oder Erfahrungswerten durch die Prüfinstanz vorzugeben, und kann hier nicht übergreifend festgelegt werden.

3.7 Inhaltsprüfung von Exportdaten

Die genaue Ausgestaltung der Inhaltsprüfung von Exportdaten wird üblicherweise von der jeweiligen Prüfinstanz vorgegeben. Dabei kann die Prüfung sich auf die Erfassung von Umsätzen beschränken oder auch die Korrelation mit anderen Datenbeständen einbeziehen.

Einige in der Betriebsprüfung genutzte statistische Verfahren (Newcomb-Benford-Analyse und Chi-Quadrat-Test für Tagesgesamtumsätze) werden keine Ergebnisse liefern, da sie der Aufdeckung frei erfundener Werte dienen. Dies kann es bei der Nutzung von INSIKA prinzipiell nicht geben.

Bei Verteilungsanalysen (z. B. Umsatzverteilungen im Tages- oder Wochenverlauf, Vorjahresvergleiche, etc.) wird die Aussagekraft durch INSIKA wesentlich erhöht. Vor allem führt die zeitweise Nichterfassung von Daten mit diesen Analyseverfahren zu Auffälligkeiten.

Die Anwendung der genannten Verfahren auf ungesicherte Daten kann auf Dauer keine zuverlässige Aufdeckung von Manipulationen mehr erlauben. Da die Verfahren bekannt sind, kann mit Hilfe von intelligenter Manipulationssoftware (sog. „Zapper“) der Datenbestand so verändert werden, dass statistische Methoden keine Manipulation mehr aufdecken können. Nur bei einer gesicherten Ursprungsaufzeichnung, wie sie bei INSIKA verwendet wird, kann jede nachträgliche Veränderung sofort erkannt werden.

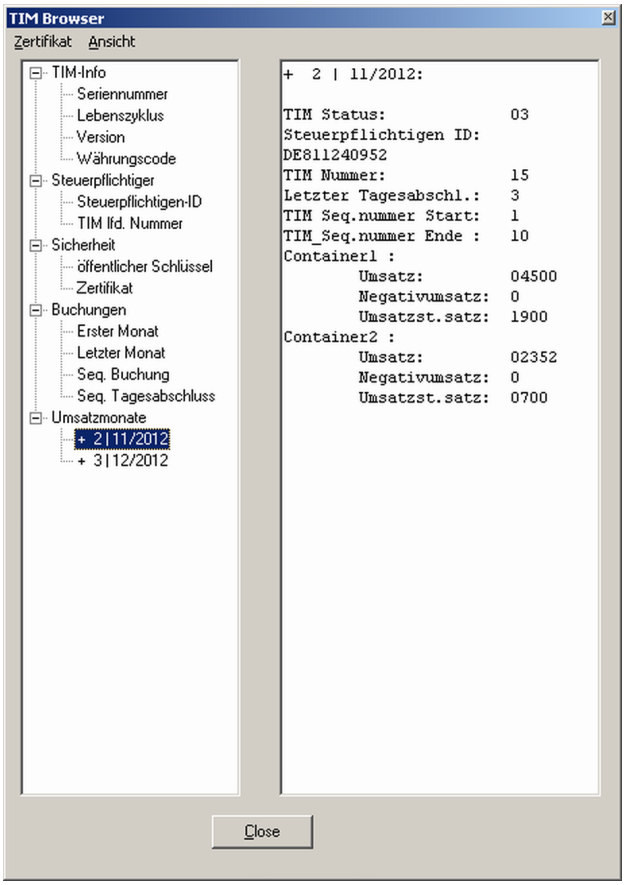


Abbildung 7: TIM-Browser

4 Auswertung von TIM-Daten

Die Auswertung der TIM-Daten kann als Sonderfall der Prüfung angesehen werden. Nur für den Fall, dass keine Exportdaten vorgelegt werden können, ist die Auswertung der TIM-Daten sinnvoll. Da die auf dem TIM gespeicherten Daten mit jedem Tagesabschluss ausgegeben werden, kann auch jeder Unternehmer diese problemlos einsehen.

4.1 Umsatzspeichermodell des TIM

Auf dem TIM werden die Umsätze in Monatssummen für jeweils sechs verschiedene Umsatzsteuerklassen gespeichert. Mit einer Buchung ließen sich somit sechs unterschiedliche Umsatzsteuersätze übertragen. Der jeweilige Umsatzsteuersatz ist dabei auf dem TIM nicht in der Höhe, sondern in der Klasse festgelegt. Für Deutschland bilden der Standardsatz, der ermäßigte Satz und die Umsatzsteuerbefreiung die üblichen Klassen [12].

Die Höhe der Umsatzsteuersätze wird erst mit einer Buchung in den entsprechenden Monatssummenspeicher eingetragen. Änderungen der Umsatzsteuersätze erfordern damit keine Änderungen auf dem

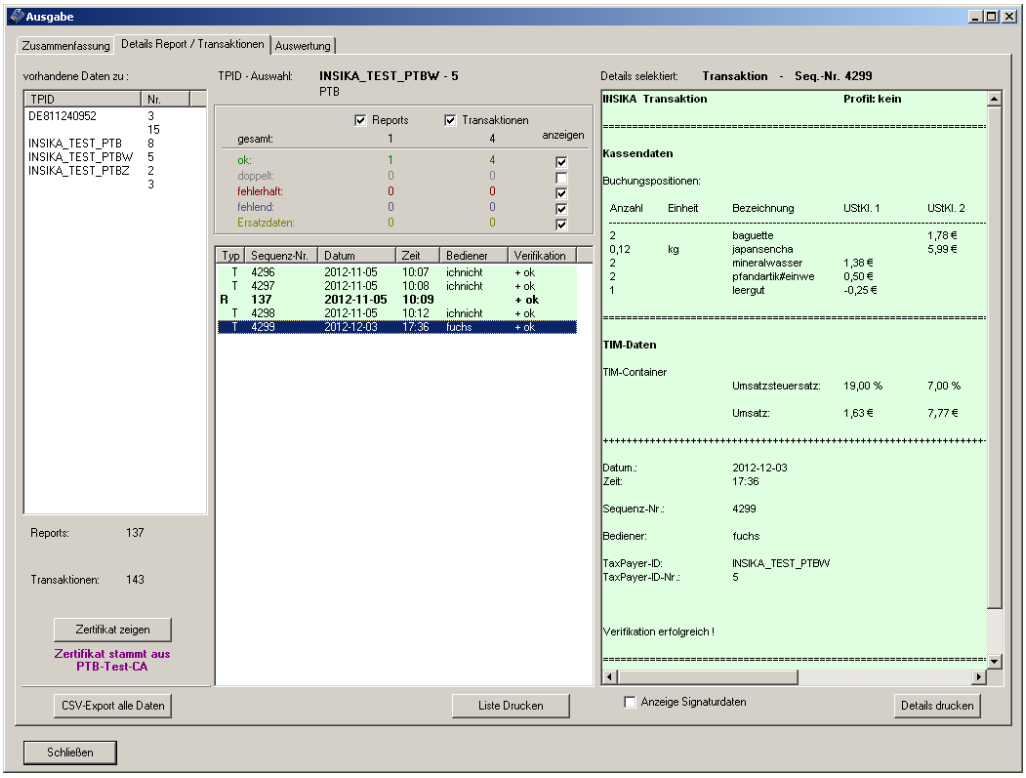


Abbildung 8: Verifikation von XML-Exportdaten mit der IVM-Software

TIM und können im laufenden Betrieb vorgenommen werden. Durch das System der sechs Umsatzsteuerklassen lassen sich zudem alle Umsatzsteuersysteme der Europäischen Union abbilden [22].

4.2 TIM-Browser

Zur Auswertung der TIM-Daten kann z. B. der an der PTB entwickelte „TIM-Browser“ genutzt werden. Wie Abbildung 7 zeigt, kann mit dieser Applikation der Inhalt des TIM ausgelesen werden. Auch lassen sich die entsprechenden Umsatzsummen ermitteln, anhand derer sich eine Abschätzung von Monatsumsätzen durchführen lässt. In einem möglichen Streitfall zwischen Unternehmer und Prüfinstanz bietet sich damit eine Grundlage zur Einigung.

5 IVM-Verifikationssoftware

An der PTB wurde im Rahmen des INSIKA-Projekts beispielhaft die Software „INSIKA Verifikations Module“ (IVM) entwickelt. Mit dieser Software lassen sich Signaturen sowohl von XML-Exportdaten als auch von gedruckten Belegen verifizieren. Bei letzteren lässt sich zusätzlich die Übereinstimmung von Buchungspositionen und Hashwert eines gedruckten Belegs prüfen (siehe 2.5). Damit steht mit dem IVM ein Werkzeug zur Verfügung, das alle INSIKA-Prüfverfahren für Belege und XML-Exportdaten abdeckt.

Neben einer eigenständigen Applikation wie dem IVM kann natürlich auch eine webbasierte Architektur zur Prüfung von XML-Exportdaten entworfen werden. Je nach Anforderung kann dabei die Signaturverifikation auf dem Server oder auf dem Client durchgeführt werden. Auch bei einer webbasierten Architektur kommt natürlich der Vertrauenswürdigkeit des Anbieters eine besondere Bedeutung zu.

5.1 IVM zur Prüfung von XML-Exportdaten

Abbildung 8 zeigt das IVM mit der Prüfung von einigen XML-Exportdaten. Enthalten sind u. a. Daten aus dem Beispiel in Abbildung 6. Die dreispaltige Ansicht zeigt das Identifikationsmerkmal, Buchungen und Tagesabschlüsse und die dazugehörigen detaillierten Inhalte. Die Ergebnisse der jeweiligen Signaturverifikation sind farbig hinterlegt. Damit stehen die Ergebnisse im Vordergrund und möglichen Fehlern lässt sich auf einfache Weise nachgehen.

Über den Export der Daten als „CSV“ stellt das IVM auch Daten für das Programmpaket „IDEA“ bereit. Diese Software dient der Datenanalyse und wird bundeseinheitlich von der deutschen Finanzverwaltung im Bereich der Betriebsprüfung verwendet [23].

5.2 IVM zur Prüfung der Zertifikatskette

Im IVM ist auch die Abfrage vom Zertifikatsserver, die Zertifikatsprüfung und der Abgleich mit der Zertifikatssperrliste integriert. Abbildung 9 zeigt beispielhaft die Verifikation der Zertifikatskette. Damit kann der Ursprung der Daten eindeutig zugeordnet werden. Die Prüfung der Zertifikatskette wird im IVM selbstverständlich automatisch durchgeführt.

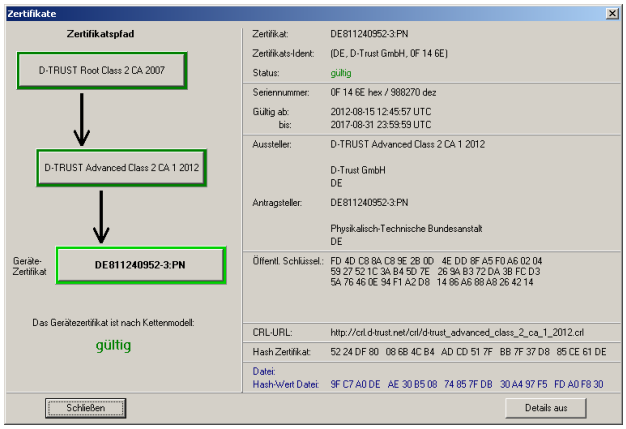


Abbildung 9: Verifikation der Zertifikatskette im IVM

6 Zusammenfassung

Im INSIKA-Konzept werden Daten an Registrierkassen und Taxametern mit Hilfe einer Smartcard gesichert. Mit Prüfverfahren können alle Veränderungen an diesen Daten sicher, schnell und automatisiert erkannt werden. Die Prüfverfahren lassen sich direkt aus dem Systemkonzept ableiten und stehen jedem frei zur Verfügung. Da das Konzept und die Spezifikationen offen zugänglich sind, können Prüfwerkzeuge von verschiedenen Anbietern bereitgestellt werden.

Im INSIKA-System lassen sich Exportdaten, gedruckte Belege und auf dem TIM gespeicherte Umsatzsummen prüfen. Den Kern der Prüfung stellt dabei die Signaturverifikation von Exportdaten und Belegen dar. Durch eine erfolgreiche Signaturverifikation wird die Integrität und Authentizität der geschützten Daten sichergestellt.

Die Konsistenz von Exportdaten lässt sich anhand der Sequenznummern nachweisen. Die Exportdaten sind durch das XML-Format einheitlich und unabhängig von Medium und Hersteller definiert. Umsatzanalysen oder weitergehende Methoden der Datenauswertung können auf gesicherte Exportdaten zurückgreifen.

Gedruckte Belege dienen nicht nur dem zeitnahen Funktionsnachweis des Systems, sie können auch zu Stichproben in den korrespondierenden Exportdaten herangezogen werden. Bei der Verwendung von 2D-Codes auf den Belegen kann die Online-Verifikation jederzeit mit vielen Mobiltelefonen und Smartphones durchgeführt werden, ohne dass dafür eine spezielle Software benötigt wird. Da die Online-Verifikation damit prinzipiell von jedem Kunden durchgeführt werden kann, könnte eine sehr hohe Prüfdichte erreicht werden.

Literatur

[1] BMF. *BMF-Schreiben vom 16. Juli 2001 - IV D 2 - S 0316 - 136/01 - Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU)*. Bundesrepublik Deutschland, Bundesministerium der Finanzen, Juli 2001. URL: `http://bundesfinanzministerium.de/`.

[2] BMF. *BMF-Schreiben vom 26.11.2010 - IV A 4 - S 0316/08/10004-07 - (2010/0946087) - Aufbewahrung digitaler Unterlagen bei Bargeschäften*. Bundesrepublik Deutschland, Bundesministerium der Finanzen, Nov. 2010. URL: `http://bundesfinanzministerium.de/`.

[3] ISO. *ISO/IEC 7816-1:1998 Identification cards - Integrated circuit(s) cards with contacts - Part 1: Physical characteristics*. International Organization for Standardization, 1998.

[4] ISO. *ISO/IEC 7816-2:1999 Identification cards - Integrated circuit(s) cards with contacts - Part 2: Dimensions and location of the contacts*. International Organization for Standardization, 1999.

[5] ISO. *ISO/IEC 7816-3:1997 Identification cards - Integrated circuit(s) cards with contacts - Part 3: Electronic signals and transmission protocols*. International Organization for Standardization, 1997.

[6] ISO. *ISO/IEC 7816-4:1995 Identification cards - Integrated circuit(s) cards with contacts - Part 4: Interindustry commands for interchange*. International Organization for Standardization, 1995.

[7] INSIKA-Projekt. *INSIKA TIM Schnittstellendokumentation*. Version T.1.0.6-02. Physikalisch-Technische Bundesanstalt, März 2010. URL: `http://insika.de/`.

[8] INSIKA-Projekt. *INSIKA TIM Schnittstellendokumentation, Zusatz*. Version T.1.1.0-01. Physikalisch-Technische Bundesanstalt, Feb. 2011. URL: `http://insika.de/`.

[9] NIST. *FIPS Publication 186-3: Digital Signature Standard (DSS)*. National Institute of Standards und Technology, Juni 2009. URL: http://csrc.nist.gov/publications/PubsFIPS.html.

[10] INSIKA-Projekt. *INSIKA Exportformat*. Version T.1.0.6-01. Physikalisch-Technische Bundesanstalt, März 2010. URL: http://insika.de/.

[11] INSIKA-Projekt. *RESTful INSIKA Interface. Schnittstelle zur Übertragung von signierten Fahrt- und Schichtdaten*. Version 0.13.5. Physikalisch-Technische Bundesanstalt, Feb. 2011. URL: http://insika.de/.

[12] BMJ. *Umsatzsteuergesetz (UStG)*. Version 07.12.2011. Bundesrepublik Deutschland, Bundesministerium der Justiz, Dez. 2011. URL: http://www.gesetze-im-internet.de/ustg_1980/index.html.

[13] BMJ. *Abgabenordnung*. Version 22.12.2011. Bundesrepublik Deutschland, Bundesministerium der Justiz, Dez. 2011. URL: http://www.gesetze-im-internet.de/ao_1977/index.html.

[14] NIST. *FIPS Publication 180-4: Secure Hash Standard (SHS)*. National Institute of Standards und Technology, März 2012. URL: http://csrc.nist.gov/publications/PubsFIPS.html.

[15] Jörg Wolff u. a. »Sicherung von Messdaten in verteilten Messsystemen«. In: *Verteilte Messsysteme*. Hrsg. von F. Puente León, K.-D. Sommer und M. Heizmann. KIT Scientific Publishing, Karlsruhe, März 2010, S. 193–205. ISBN: 978-3-86644-476-8. DOI: 10.5445/KSP/1000015670.

[16] Rat der Europäischen Union. *Richtlinie 2004/22/EG des Europäischen Parlaments und des Rates vom 31. März 2004 über Messgeräte*. Amtsblatt der Europäischen Union L135 vom 30.04.2004. März 2004. URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004L0022:DE:NOT.

[17] INSIKA-Projekt. *INSIKA Profil Taxameter*. Version T.1.1.0-10. Physikalisch-Technische Bundesanstalt, Feb. 2011. URL: http://insika.de/.

[18] S. Josefsson. *RFC4648: The Base16, Base32, and Base64 Data Encodings*. The Internet Engineering Task Force (IETF), Okt. 2006. URL: http://tools.ietf.org/html/rfc4648.

[19] ISO. *ISO/IEC 18004:2006 Information technology - Automatic identification and data capture techniques - QR Code 2005 bar code symbology specification*. International Organization for Standardization, 2006.

[20] *Extensible Markup Language (XML) 1.0 (Fifth Edition). W3C Recommendation 26 November 2008*. World Wide Web Consortium (W3C). Nov. 2008. URL: http://www.w3.org/TR/xml/ (besucht am 24. 04. 2012).

[21] *XML Schema Part 0: Primer Second Edition. W3C Recommendation 28 October 2004*. World Wide Web Consortium (W3C). Okt. 2004. URL: http://www.w3.org/TR/ (besucht am 24. 04. 2012).

[22] Rat der Europäischen Union. *Richtlinie 2006/112/EG des Rates vom 28. November 2006 über das gemeinsame Mehrwertsteuersystem*. Amtsblatt der Europäischen Union L347 vom 11.12.2006. Dez. 2006. URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0112:DE:NOT.

[23] BMF. *Information zum „Beschreibungsstandard für die Datenträgerüberlassung“*. Version 15.08.2002. Bundesrepublik Deutschland, Bundesministerium der Finanzen, Aug. 2002. URL: http://bundesfinanzministerium.de/.