INSIKA
TIM Schnittstellendokumentation
V.2.1.0

Revision: 00

Letzte Änderung: 27.06.2017

Status: freigegeben

Hinweis zum Dokument

Diese INSIKA-Dokumentation enthält die Festlegungen des Arbeitskreises INSIKA des ADM e.V. für die TIM-Schnittstelle. Mit der Veröffentlichung der Dokumentation können sich Interessierte über die Grundlagen der INSIKA-Technik informieren und sind damit in der Lage, das Verfahren praktisch umzusetzen. Um schnell über Änderungen informieren zu können, wird die Dokumentation nur an registrierte Unternehmen ausgegeben.

Aus den in dieser Beschreibung dargestellten technischen Inhalten können keine Garantien oder Verpflichtungen abgeleitet werden. Die Autoren und das Konsortium übernehmen bei Übernahme oder Benutzung des Verfahrens oder von Teilen davon keine Haftung oder Verantwortung.

Eine entwicklungsbegleitende Unterstützung von Implementierungen ist momentan nicht möglich. Fragen zum Verfahren werden im Rahmen der Möglichkeiten beantwortet.

Weitere Informationen: http://www.insika.de/

Das INSIKA-Projekt wurde vom Bundesministerium für Wirtschaft und Technologie unter dem Kennzeichen MNPQ 11/07 gefördert.

Änderungshistorie

Version	Datum	Änderungen
0.9	30.05.2008	Initiale Version
0.9.27	10.03.2009	Veröffentlichung durch Versand an alle registrierten Unternehmen
T106-02	09.03.2010	Veröffentlichung an registrierte Unternehmen
T110-01	06.08.2014	Review und Aktualisierung, Integration Nachtrag für Version 1.1.0
T110-02	19.03.2015	Profil Registrierkasse in separates Dokument verschoben, diverse Details präzisiert, Review
V.2.0.0-00	14.12.2016	Veröffentlichung an registrierte Unternehmen Veränderungen gegenüber der Vorversion: • Alternative Signaturlänge ECDSA-256 mit SHA-256, Neue Transaction-Befehle für Sonderanwendungen, • Neuer Befehl GET LATEST RESPONSE, • Signatur von Nullumsätzen möglich • Veränderungen bei der Behandlung von Umsätzen aus Agenturgeschäft und Lieferschein
V.2.1.0-00	27.06.2017	Veröffentlichung an registrierte Unternehmen Veränderungen gegenüber der Vorversion: • Einführung zusätzlicher Fehlercodes • Anzeige langer Reports (>256 Byte) • Erweiterung GET DATA TIM Status extended • Neuer Befehl GET DATA Memory Status

Autoren:	Mathias Neuhaus (cryptovision GmbH) Jörg Wolff (PTB [bis 2013]) Norbert Zisky (ADM, PTB [bis 2015]))
Titel:	INSIKA TIM Schnittstellendokumentation
Referenziertes TIM-Package:	V.2.1.0
Revision:	00
Status:	freigegeben
Letzte Änderung:	27.06.2017
Dateiname:	INSIKA_TIM_Interface-V210-00-de.docx
Anzahl der Seiten:	89
Kontakt:	http://insika.de/de/kontakt

Inhaltsverzeichnis

Tabellenverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

Abkürzung	Erläuterung
AID	Application IDentifier (ISO 7816-5)
APDU	Application Protocol Data Unit (ISO 7816)
ASCII	American Standard Code for Information Interchange
ASN.1	Abstract Syntax Notation One
ATR	Answer to Reset (ISO 7816-3)
BCD	Binary Coded Decimal
BER	Basic Encoding Rules (ASN.1)
BP	hier: Buchungsposition (= ITEM)
CLA	Class-Byte, Teil der ISO 7816 Befehls APDU
DER	Distinguished Encoding Rules (ASN.1)
DF	Dedicated File (ISO 7816-4)
ECDSA	Elliptic Curve Digital Signature Algorithm
ECC	Elliptic Curve Cryptography
EF	Elementary File (ISO 7816-4)
FID	File Identifier (ISO 7816-4)
ID	IDentifikation
INS	Instruction, Teil der ISO 7816 Befehls APDU
ITEM	Item, Buchungsposition (= BP)
LC	Length Command, Teil der ISO 7816 Befehls APDU
LE	Length Expected, Teil der ISO 7816 Befehls APDU
MF	Master File (ISO 7816-4)

Abkürzung	Erläuterung
MSB	Most Significant Bit
OID	Object Identifier
P1, P2	Parameter 1 und 2, Teil der ISO 7816 Befehls APDU
PIN	Personal Identification Number
PIX	Propritary application Identifier eXtension (ISO 7816-5)
RID	Registered IDentifier (ISO 7816-5)
SFID	Short File ID
SHA-1	Secure Hash Algorithm (FIPS 180-1)
SHA-256	Secure Hash Algorithm (FIPS 180-4)
SW1, SW2	Status Word 1 und 2 (ISO 7816)
TIM	Tax Identification Module
TLV	Tag-Length-Value (BER-TLV)
TP ID	Tax Payer IDentification, Identifikationsmerkmal
USt-IdNr	Umsatzsteuer-Ident-Nummer
VAT	Value Added Tax, Umsatzsteuer
WID	Wirtschaftsidentifikations-nummer

Glossar

Agenturgeschäft / Third-party turnover	Bei Agenturumsätzen handelt es sich um Lieferungen oder Leistungen im Namen und auf Rechnung eines Dritten, die aber trotzdem auf dem Beleg abgedruckt werden. Bei einer Prüfung ist nachzuweisen, dass die Umsätze durch den Dritten versteuert wurden.
ANSI X9.62	American National Standards Institute: Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA)
Ausgebene Stelle	Organisation, die mit der Aufgabe der Kartenausgabe beauftragt ist. Dazu gehören die Aufgaben einer CA (Certificate Authority = Zertifizierungsstelle), also z.B. die Prüfung von Anträgen, das Erzeugen und Verwalten der kryptografischen Zertifikate, aber auch spezielle Leistungen wie z.B. ein besonderer Zugriff der Finanzbehörden auf die Datenbestände
Buchung	Verkaufsvorgang, i.d.R. bestehend aus mehreren Buchungspositionen, wird durch den Befehl TRANSACTION ausgeführt
Container	Hier: zusammengesetztes TLV-Objekt für Umsatzdaten,
FIPS 180	National Institute of Standards and Technology (NIST): Federal Information Processing Standards Publication 180, Secure Hash Standard (SHS), (u.a. Definition von SHA-1)
FIPS 180-4	National Institute of Standards and Technology (NIST): Federal Information Processing Standards Publication 180, Secure Hash Standard (SHS), (u.a. Definition von SHA-256)
FIPS 186	National Institute of Standards and Technology (NIST): Federal Information Processing Standards Publication 186, Digital Signature Standard (DSS), (u.a. Definition von ECDSA)
Hash, Hashwert	Ergebnis einer kryptografischen Einwegfunktion, genauer: kryptografischen Hashfunktion, im ECDSA-192-Modus SHA-1 und im ECDSA-256-Modus SHA-256
INSIKA	Projektname, INSIKA = INtegrierte SIcherheit für messwertverarbeitende KAssensysteme
ISO/IEC 7816	International Organization for Standardization and the International Electrotechnical Commission, Information technology – Identification cards – Integrated circuit(s) cards with contacts (Standard für elektronische ID Karten, insbesondere Smart Cards)
ITU-T X.509v3	International Telecommunication Union - Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks (Standard für elektronische Zertifikate)

ITU-T X.690	International Telecommunication Union - Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER), (auch in der ISO/IEC 8825-1 standardisiert)
Lieferschein / Delivery note	Abgabe von Waren bzw. Erbringung von Leistungen, für die erst später eine Rechnung erstellt wird, die aber trotzdem in abgesicherter Form dokumentiert werden sollen .
Negativumsatz / Negative Turnover	Negative Anteile des Umsatzes einer Buchung. Negativumsätze werden als positive Werte übertragen.
Personalisierung	Durch die ausgebende Stelle vor Ausgabe des TIM durchgeführt, umfasst Eintragen der Daten nach → 8.1, Generierung des Schlüsselpaares auf dem TIM, Ausstellung und Aufbringen des Zertifikats
Positivumsatz / Positive Turnover	Positive Anteile des Umsatzes einer Buchung. Positivumsätze werden nicht getrennt übertragen. Es gilt der Zusammenhang: Umsatz = Positivumsatz - | Negativumsatz |
Private Key / privater Schlüssel	Privater (und geheimer) Teil des Schlüsselpaares des TIM, wird zur Signaturerstellung verwendet, nicht lesbar, verlässt das TIM niemals
Profil	Hier: auf einen speziellen Einsatzbereich abgestimmte Definition, welche die Abbildung von Buchungspositionen umfasst (→ 1.4)
Public Key / öffentlicher Schlüssel	Öffentlicher Teil des Schlüsselpaares des TIM, nötig zur Signaturverifikation
REPORT	Befehl an das TIM, mit dem die Umsatzspeicher des TIM zurückgegeben werden. Der Befehl führt einen sog. Tagesabschluss durch.
Sequenznummer	Streng monoton aufsteigende Nummer, wird durch das TIM vergeben
Signatur	Elektronische Signatur, wird durch das TIM berechnet
Smart Card	Chipkarte ohne die für INSIKA nötige Software (TIM-Package)
Tagesabschluss	wird durch den Befehl REPORT ausgeführt
Tax-Identification-Module (TIM)	Smart Card mit INSIKA Software ("TIM-Package")
TIM-Package	Softwarepaket auf der Smart Card, das die speziellen INSIKA-Funktionalitäten bereitstellt
TLV-Objekt	Hier: Datenobjekt, bei dem den eigentlichen Daten ("Value") ein Byte zur eindeutigen Bezeichnung ("Tag") und ein Byte als Längenfeld ("Length") vorangestellt werden (siehe auch "Use of the Basic Encoding Rules" in ISO/IEC 7816-4 Annex D).

Training	Buchungen, die ausschließlich zu Übungs- und Testzwecken durchgeführt werden. Dabei handelt es sich auch nicht um steuerpflichtige Umsätze.
TRANSACTION	Befehl an das TIM, mit dem Daten einer Buchung an das TIM übergeben werden. Bei positiver Plausibilisierung wird eine Signatur zurückgegeben.
Umsatz / Turnover	Umsatzsteuerbezogenes Entgelt einer Buchung (und damit die Summe der einzelnen Preise der Buchungspositionen einer Buchung); wird immer auf eine Umsatzsteuerklasse bezogen; kann brutto oder netto an das TIM übergeben werden; monetäre Einheit
Umsatzspeicher	Speicher für verschiedene Beträge und Mengen auf dem TIM, die zu Erfassung von Summendaten dienen. Aus den Umsatzspeichern werden die Berichte (Befehl REPORT) erstellt.
Umsatzsteuer / Value Added Tax (VAT)	Hier: (umsatz-)steuerlicher Anteil am Entgelt einer Buchung; hier monetäre Einheit
Umsatzsteuerklasse	Von aktuellen Umsatzsteuersätzen unabhängige Definition, wird vom jeweiligen aktuell gültigen Umsatzsteuersatz ausgefüllt
Umsatzsteuersatz / VAT Rate	Prozentualer Satz der Umsatzsteuer
Umsatzüberlauf	Wenn der Maximalwert eines Umsatzzählers auf dem TIM überschritten wird (im Regelbetrieb nicht möglich) weist der Zähler danach einen zu niedrigen Wert aus (Beispiel: Läge der Maximalwert bei 1000, würde ein Wert von 1015 als 15 gespeichert). Um diese Situation zu erkennen, wird in diesem Fall die Tatsache des Überlaufs beim Abruf des Wertes oder einer darauf basierenden Summe angezeigt.
Zertifikat	Hier: elektronisches Zertifikat, durch die ausgebende Stelle signierte Datei, siehe auch X.509v3

1 Allgemeine Informationen

1.1 Änderungsangaben

1.1.1 Änderungen zur Version T.1.1.0

Diese Version der Spezifikation wurde unter folgenden Maßgaben entwickelt:

- Erschließung weiterer Anwendungsbereiche für INSIKA
- Anpassung an aktuelle kryptographische Verfahren und Schlüssellängen
- Verbesserte Abbildung spezieller Sachverhalte (Lieferschein- und Agenturgeschäfte)

Änderungen im Datenmodell wurden aus Kompatibilitätsgründen nicht vorgenommen und waren auch nicht erforderlich. Gegenüber der Vorversion (T.1.1.0) ergeben sich die hier beschriebenen wesentlichen Änderungen.

Aufgrund der spezifischen Anforderungen aus den angestrebten Einsatzbereichen wurden zusätzliche Varianten des TRANSACTION Befehls definiert. Auch der Befehl VERIFY wurde passend erweitert.

Die Fixierung auf einen einzigen Signaturalgorithmus wurde aufgehoben. Zusätzlich zu den bisherigen Parametern (ECC, 192 bit NIST, SHA-1) ist ein weiterer Parametersatz verfügbar (ECC, 256 bit NIST, SHA-256). Die Auswahl erfolgt zum Zeitpunkt der Personalisierung. Die konkret verwendete Variante kann (indirekt) über die Befehle GET DATA Hash Length oder direkt über GET DATA Cryptographic Algorithms ermittelt werden.

Eine wesentliche Veränderung betrifft die Behandlung von Agenturgeschäften. Diese werden jetzt umsatzsteuersatzbezogen mit in den Umsatz-Containern E1h…E6h übergeben; die Übergabe im bisherigen Container E7h entfällt. Der Container E7h wird nur vom TIM unter Verwendung der übergebenen Umsätze verwaltet. Für alle Einsatzfälle, die bisher auf die Umsätze aus Agenturgeschäften) verzichtet haben, ergeben sich aber keinerlei Änderungen! Die INSIKA-Profile Kassen und Taxi werden soweit erforderlich angepasst.

Zusätzlich wurden erkannte Fehler behoben, sowie einige Abschnitte präziser formuliert.

1.1.2 Änderungen zur Version 2.0.0

Die maximal mögliche Länge der Antwort auf einen REPORT Befehl erfordert die Unterstützung von „extended Length“ APDUs, siehe ISO 7816-4. Deshalb wurde die Meldung 98 D1h eingeführt. Weiterhin wurden Fehlercodes 98 D2h und 98 F2h ergänzt. Bei Auftreten der Fehler 98 E1h, 98 E2h und 98 F2h wird das TIM automatisch deaktiviert. Es wurde der Befehl GET DATA TIM Status extended erweitert und GET DATA Memory Status spezifiziert. Alle Änderungen und Ergänzungen haben keine Auswirkungen auf bestehende Implementierungen.

1.2 Dokumentinformationen.

Dieses Dokument beschreibt die Schnittstelle der INSIKA Smart Card, nachfolgend „TIM“ (Tax-Identification-Module) genannt. Mit diesem Dokument lässt sich die TIM-Schnittstelle in ein Kassensystem und weitere Anwendungsumgebungen integrieren. Dafür stehen der Anwendungsumgebung angepasste Profilspezifikationen in separaten Dokumenten zur Verfügung.

Der Wechsel der Kennung der TIM-Schnittstellendokumentation von „T“ auf „V“ ergibt sich aus dem Übergang aus der Testphase zum Realbetrieb. Die TIM-Karten T.xx werden seit 2010 in unterschiedlichen Anwendungsbereichen erfolgreich eingesetzt. Probleme mit der Hardware oder Software sind nicht bekannt.

Kenntnisse von Smart-Card-Schnittstellen und den in diesem Bereich genutzten Begriffen werden vorausgesetzt. Es werden ausschließlich Informationen dargestellt, die für eine Implementierung der TIM-Schnittstelle nötig sind. Die interne Arbeitsweise des TIM ist in diesem Dokument nicht spezifiziert. Kenntnisse des INSIKA-Verfahrens sind zum Verständnis nötig.

1.2.1 Struktur des Dokuments

Das Dokument ist folgendermaßen strukturiert:

Kapitel 1 enthält allgemeine Informationen zum Dokument und zur Smart Card.

Kapitel 2 dokumentiert die auf der Schnittstelle übertragenen Datenobjekte erst allgemein und anschließend in der Reihenfolge ihrer Struktur (Tag-Length-Value).

Kapitel 3 legt die INSIKA Befehle dar, die an das TIM gesendet werden können.

Kapitel 4 enthält die Fehlercodes, die in der Antwort auf einen Befehl vom TIM zurückgegeben werden können.

Kapitel 5 erläutert den Lebenszyklus des TIM.

Kapitel 6 enthält Definitionen zu Umsatzsteuerklassen, Zeichenersetzung und Rundung.

Kapitel 7 legt alle Informationen dar, die für eine Signaturverifikation nötig sind.

Kapitel 8 erläutert alle Daten, die auf dem TIM gespeichert sind.

Kapitel 9 erläutert das Konzept der INSIKA-Profile.

Der Anhang (→ 10) enthält Beispiele und zugehörige Erläuterungen.

Kapitel 1 – 6 und das Dokument mit dem der Anwendung entsprechenden Profil sind Grundvoraussetzung für eine Basis-Integration der INSIKA-Technik in ein System. Soll eine vollständige Implementierung vorgenommen werden, sind zusätzlich die Kapitel 7 und 8 zu beachten.

1.2.2 Sprache

In diesem Dokument sind Namen und Erläuterungen in deutscher Sprache verfasst. Bezeichner von Datenobjekten ("Tags"), Befehle und Fehlercodes werden in Englisch definiert. Sie werden auch unverändert in Übersetzungen des Dokuments übernommen.

1.2.3 Hexadezimale Darstellung

Die hexadezimale Darstellung von Bytes wird durch den Anhang eines kleinen "h" kenntlich gemacht: xxh, xx xxh hexadezimale Darstellung des Bytes xx bzw. der Bytes xx xx.

1.2.4 Verwendung von Präfixen

Das Präfix "TIM" bezeichnet Datenobjekte, die in der direkten Kommunikation mit dem TIM verwendet werden, d.h. diese Datenobjekte werden direkt im Feld "Data" der ISO 7816 – APDUs verwendet.

Datenobjekte mit anderen Präfixen (z.B. "ITEM") sind in Profilen festgelegt und werden nicht direkt auf der TIM-Schnittstelle verwendet. Einzige Ausnahme bildet dabei der optional verwendbare Befehl HASH, bei dem jedes Datenobjekt übergeben werden kann.

1.3 Kryptografische Verfahren

Das INSIKA-Verfahren legt zur Datensicherung digitale Signaturen mit dem Kryptographieverfahren ECDSA gemäß ANSI X9.62 auf dem Grundkörper GF(p) fest. Aktuell werden als Hashverfahren SHA-1 gemäß FIPS 180-1 mit 160 bit und ECDSA mit einer Schlüssellänge von 192 bit verwendet. Die gemäß Spezifikation Version T.1.1.0 ausgelieferten INSIKA-Karten (TIM) unterstützen nur diese Schlüssellänge.

INSIKA-Karten gemäß dieser Spezifikation unterstützen mit ECDSA-256 und SHA-256 eine größere Schlüssellänge. Der Übergang auf längere Signaturschlüssel folgt den Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Die TIM-Karten gemäß dieser Spezifikation unterstützen beide Schlüssellängen. Dabei ist allerdings bei der Beantragung der Karte aus technischen Gründen die Angabe der Schlüssellänge erforderlich. Nach Produktion und Auslieferung der Karte kann während der Laufzeit die Signaturschlüssellänge nicht verändert werden. Es wird folglich ein ECDSA-192- und ECDSA-256-Modus unterschieden.

1.4 Konzept der INSIKA Profile

INSIKA Profile dienen der Abbildung anwendungsspezifischer Daten eines Systems. Ein Profil definiert die Datenobjekte, über die der Hashwert der Buchungspositionen gebildet wird. Im Rahmen einer Buchung wird dieser Hashwert (→ 2.6.9) an das TIM übergeben und signiert (→ 3.4).

Die Datenobjekte eines Profils (Buchungspositionen) werden nicht direkt im Rahmen einer Buchung an das TIM übergeben. Da jedoch der Hashwert dieser Datenobjekte signiert wird, gehen auch diese Datenobjekte (indirekt) in die Signatur mit ein. Somit kann eine große Zahl von Datenobjekten in die Signatur eingehen, ohne dass diese auf der TIM Schnittstelle übertragen werden müssen. Bei Veränderungen an Profilen bleibt das TIM unverändert.

Durch das Konzept der Profile ist es möglich, das INSIKA System auf unterschiedliche Anwendungen anzupassen. Insbesondere lassen sich hiermit verschiedene Systeme abbilden. In jeder Anwendung wird genau ein Profil verwendet.

Das Kapitel 9 enthält weitere Erläuterung zum Konzept der Profile. Für eine Implementierung ist immer die separate Dokumentation des jeweiligen Profils erforderlich.

1.5 Format der Smart Card

Das TIM wird im Format ID-1 nach ISO 7816 ausgeliefert. Die Smart Card ist so perforiert, dass sie sich durch Ausbrechen in das ID-000 oder MicoSim-Format verwandeln lässt. Die Kontaktbelegung ist in der ISO 7816-2 festgelegt.

1.6 Elektrische Eigenschaften

Die elektrischen Eigenschaften des TIM folgen der ISO 7816-3. Das TIM V.2.1.0 ist eine Smart Card der Klasse A und B und damit im Bereich Vcc = 2,7..5,5 V nutzbar (siehe ISO 7816-3).

1.7 Übertragungsprotokoll / Kartenleser

Die Datenübertragung zum / vom TIM erfolgt mit Protokoll T=1 (ISO 7816-3). Die Unterstützung von „extended Length“ APDUs ist erforderlich. Damit kann das TIM mit Hilfe von PC-Kartenlesern, ISO 7816 Schnittstellen-ICs oder direkt angesteuert werden. Bei PC-

Kartenlesern ist ein Modell der Klasse 1 vollkommen ausreichend, ein PIN-Pad ist nicht nötig.

Eine physische Integration des Kartenlesers (mit dem TIM) in das jeweilige System ist keine Voraussetzung. So ist z.B. eine Kommunikation mit dem TIM über ein (Funk-) Netzwerk denkbar, um INSIKA auf Geräten zu nutzen, in die ein Kartenleser nicht direkt integriert werden kann.

2 Datenobjekte

2.1 TLV Kodierung

Alle Daten, die im Feld "Data" der ISO 7816 - APDUs abgelegt sind, werden im TLV-Format übertragen. Dazu werden den eigentlichen Daten (VALUE → 2.6) ein Byte zur eindeutigen Bezeichnung (TAG → 2.4) und ein Byte für die Länge (LENGTH → 2.5) vorangestellt. Das gesamte Datenobjekt wird nachfolgend TLV-Objekt genannt. Das hier verwendete BER-TLV ist identisch zum "SIMPLE-TLV".

2.2 Zusammengesetzte Datenobjekte

Datenobjekte können aus mehreren Unterelementen zusammengesetzt werden. Zusammengesetzte Datenobjekte werden zur Unterscheidung von einfachen Datenobjekten („primitive DO“) als „constructed DO“ bezeichnet. Zusammengesetzte Datenobjekte lassen sich verkürzt als "verschachtelte TLV-Objekte" beschreiben.

In Abbildung 2-1 ist ein zusammengesetztes Datenobjekt mit drei Datenobjekten dargestellt. L_C gibt dabei die Gesamtlänge aller enthaltenen einfachen Datenobjekte (hier: P1, P2 und P3) inklusive der zugehörigen TL-Kodierung an.

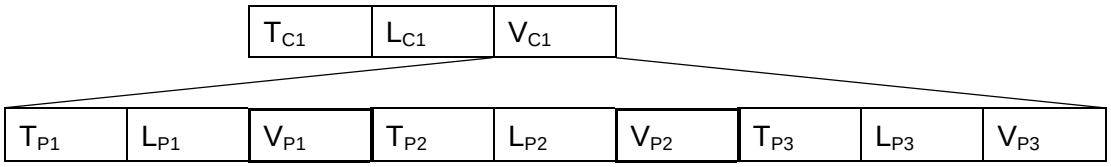

Abbildung 2-1: Zusammengesetztes Datenobjekt

Zusammengesetzte Datenobjekte werden beim TIM für die Übertragung von Umsätzen benutzt. Dabei bilden sog. Container das "constructed DO" und die enthaltenen Umsatzdaten "primitive DOs"

2.3 Datentypen

Die Datentypen gemäß Tabelle 2-1 werden in den Nutzdaten, also im Feld VALUE der TLV-Objekte verwendet. Die Anzahl der verwendeten Oktetts ist abhängig vom jeweiligen TLV-Objekt und im Abschnitt → 2.6 definiert.

Tabelle 2-1: Definition der Datentypen

Bezeichnung des Datentyps	Wertebereich (für ein Oktett)		Bemerkung
	hexadezimal	dezimal	
binär	00h..FFh	0..255	Vorzeichenlos
ASCII	20h..7Fh	32..127	druckbare Zeichen (durch die sog. Zeichenersetzung teilweise weiter eingeschränkt → 6.2)
unsigned BCD	00h..99h	0..99	hier ausschließlich "Packed BCD"
signed BCD	9Dh..0Ch..9Ch	-9..0..+9	gilt nur für das niederwertigste Byte, alle anderen Bytes analog dem Typ "unsigned BCD"

2.3.1 Binär

Binäre Werte werden vorzeichenlos, mit dem höchstwertigen Bit zuerst übertragen (MSB first).

Sofern die Länge der Nutzdaten variabel definiert ist, müssen führende Null-Bytes unterdrückt werden. Ist die Länge der Nutzdaten fest vorgeschrieben, dürfen führende Null-Bytes nicht unterdrückt werden.

2.3.2 ASCII

Text-Inhalte werden ASCII-codiert übertragen. Dabei wird ausschließlich der Wertebereich druckbarer Zeichen von 20h bis 7Fh verwendet. Um gedruckte Zeichen zurückgewinnen zu können, wird dieser Wertebereich in bestimmten Datenobjekten durch eine Zeichenersetzung weiter eingeschränkt (→ 6.2).

2.3.3 Unsigned BCD

BCD-Werte des Typs "unsigned BCD" werden als Packed BCD (also mit zwei Dezimalstellen pro Byte) übertragen. Das Byte der höchstwertigen Stelle wird zuerst übertragen. Bei einer ungeraden Stellenzahl ist das höherwertige Nibble des ersten Bytes Null (also z.B.: 0xh yzh).

2.3.4 Signed BCD

BCD-Werte des Typs "signed BCD" werden als Packed BCD (also mit zwei Dezimalstellen pro Byte) übertragen. Das Byte der höchstwertigen Stelle wird zuerst übertragen. Bei einer ungeraden Stellenzahl ist das höherwertige Nibble des ersten Bytes Null (also z.B.: 0xh yzh).

Das Vorzeichen wird im niederwertigsten Nibble gespeichert. Die Kodierung des Vorzeichens erfolgt als C – positiv oder D – negativ; alle anderen Kodierungen (0..B, E, F) sind ungültig. Der Wert Null ist mit positivem Vorzeichen definiert: 0Ch.

Führende Null-Bytes sind nicht erlaubt und müssen unterdrückt werden.

2.4 TAG (Bezeichner)

In Tabelle 2-2 sind die TAG für die TLV-Objekte des TIM definiert (aufsteigend nach dem numerischen Wert der Tags geordnet):

Tabelle 2-2: Zusammenfassung der definierten TLV-TAGs

Name	Tag	Beschreibung	Nutzdaten		ÜRichtg	
			Länge (Byte)	Datentyp (→ 2.3)	Anfrage	Antwort
TIM_SIGNATURE	9Eh	TIM Signatur (Buchung oder Tagesabschluss) → 2.6.1	48/ 64[1]	binär	X[2]	X

[1] Bei der Beantragung von INSIKA-Karten kann bzgl. der kryptografischen Algorithmen ausgewählt werden, ob die Karte a) mit ECDSA-192/SHA-1 (Signatur: 48 Bytes, Hashwert: 20 Byte) oder b) mit ECDSA-256/SHA-256 (Signatur: 64 Bytes, Hashwert: 32 Byte) arbeiten soll. Bei der neuen Kartengeneration ist Variante b) die Standardkonfiguration.

[2] Wird nur bei Verwendung des optionalen Befehls VERIFY SIGNATURE (→ 3.6) zum TIM übergeben.

Name	Tag	Beschreibung	Nutzdaten		ÜRichtg	
			Länge (Byte)	Datentyp (→ 2.3)	Anfrage	Antwort
TIM_LIFECYCLE	C0h	TIM Lebenszyklus → 2.6.2	1	binär		X
TIM_SERIAL_NO	C1h	TIM Seriennummer → 2.6.3	*[3]	*		X
TIM_VERSION	C2h	Version der TIM-Applikation, → 2.6.4	7.. 10	ASCII		X
TIM_TRANSPORT_PIN [4]	C3h	TIM Transport-PIN → 2.6.5	6	ASCII	X	
TIM_TP_ID	C4h	TIM Steuerpflichtigen-ID (Tax Payer IDentification) → 2.6.6	1..32	ASCII	X	X
TIM_TP_ID_NO	C5h	Lfd. Nummer des TIM bezogen auf eine TP_ID (Tax Payer IDentification Number) → 2.6.7	1..4	binär	X	X
TIM_OPERATOR	C6h	TIM Bediener-ID → 2.6.8	1.. 16	ASCII	X	
TIM_HASH_ TRANSACTION_ITEMS	C7h	TIM Hashwert der Buchungspositionen → 2.6.9	20/ 32[5]	binär	X	
TIM_CURRENCY	C8h	TIM Währungscode → 2.6.11	2	binär	X	
TIM_VAT_ADDON	C9h	TIM Merker exkl. Steuer → 2.6.13	0	-	X	
TIM_TRAINING	CAh	TIM Merker Training → 2.6.13	0	-	X	
TIM_SEQ_NO_ TRANSACTION	CBh	TIM Sequenznummer einer Buchung → 2.6.14	1..4	binär	X[6]	X
TIM_SEQ_NO_ REPORT	CCh	TIM Sequenznummer eines signierten Tagesabschlusses → 2.6.14	1..4	binär		X

[3] Länge und Format der Seriennummer ist von der zugrunde liegenden Smart Card abhängig.

[4] Die Verwendung der Transport-PIN ist optional. Je nach Verwendung der Transort-PIN wird das TIM im Lebenszyklus TIM_PERSONALISED oder TIM_ACTIVATED an den Steuerpflichtigen ausgeliefert.

[5] Hashwertlänge vom Modus abhängig, siehe Fußnote 1

[6] Wird nur bei Verwendung des optionalen Befehls VERIFY SIGNATURE (→ 3.6) zum TIM übergeben.

Name	Tag	Beschreibung	Nutzdaten		ÜRichtg	
			Länge (Byte)	Datentyp (→ 2.3)	Anfrage	Antwort
TIM_DATE	CDh	TIM Datum → 2.6.15	3 / 4	un-signed BCD	X	X
TIM_TIME	CEh	TIM Uhrzeit → 2.6.16	2	un-signed BCD	X	X
TIM_MONTH	CFh	Liste von Monaten, als Off-set zum ersten Monat in den gebucht werden kann → 2.6.17	0..12 1	binär		X
TIM_MONTH_START	D0h	TIM Datum, erster Monat der Umsatzperiode → 2.6.15	3	un-signed BCD	X	
TIM_MONTH_END	D1h	TIM Datum, letzter Monat der Umsatzperiode → 2.6.15	3	un-signed BCD	X	
TIM_SEQ_NO_ TRANSACTION_FIRST	D2h	TIM Sequenznummer der ersten Buchung einer Um-satzperiode → 2.6.14	1..4	binär		X
TIM_SEQ_NO_ TRANSACTION_LAST	D3h	TIM Sequenznummer der letzten Buchung einer Um-satzperiode → 2.6.14	1..4	binär		X
TIM_HASH_ REPORT_ITEMS	D4h	TIM Hashwert der Tagesab-schluss-Positionen → 2.6.10	20/ 32[7]	binär	X	
TIM_COUNTRY_CODE	D5h	Länderkennzeichen → 2.6.12	2	binär		X
TIM_ TURNOVER _ THIRDPARTY	D6h	Umsatz Agenturgeschäft → 2.6.18	1..6	signed BCD	X	
TIM_ DELIVERYNOTE	D7h	TIM Merker Lieferschein → 2.6.13	0	-	X	
TIM_TURNOVER	D8h	TIM Umsatz → 2.6.18	1..6 ..11[8]	signed BCD	X	X
TIM_TURNOVER_ NEGATIVE	D9h	TIM Negativumsatz → 2.6.18	1..6 ..11[9]	signed BCD	X	X

[7] Hashwertlänge vom Modus abhängig, siehe Fußnote 1

[8] bei Anfrage 1..6 Byte Länge, bei Antwort 1..11 Byte Länge

[9] bei Anfrage 1..6 Byte Länge, bei Antwort 1..11 Byte Länge

Name	Tag	Beschreibung	Nutzdaten		ÜRichtg	
			Länge (Byte)	Datentyp (→ 2.3)	Anfrage	Antwort
TIM_TURNOVER_ VAT	DAh	TIM Umsatzsteuer → 2.6.18	1..6	signed BCD	X	X
TIM_TURNOVER_ VAT_RATE	DBh	TIM Umsatzsteuersatz → 2.6.19	1..2	un-signed BCD	X	X
TIM_TURNOVER_ COUNTER	DCh	TIM Zähler der Buchungen → 2.6.20	1..4	binär		X
TIM_TURNOVER_ OVERFLOW	DDh	TIM Merker Umsatzüberlauf → 2.6.12	0	-		X
TIM_TURNOVER_ VAT_CHANGED	DEh	TIM Merker Änderung Umsatzsteuersatz → 2.6.13	0	-		X
TIM_CONTAINER_ VAT_1 … TIM_CONTAINER_ VAT_6	E1h .. E6h	TIM Container 1..6 (entsprechend dem Umsatzsteuersatz 1..6) → 2.6.21	6.. 34	(TLV-Obj.)[10]	X	X
TIM_CONTAINER_ THIRDPARTY	E7h	TIM Container Agenturgeschäft (“third-party”) → 2.6.21	3.. 23	(TLV-Obj.)	X	X
TIM_CONTAINER_ DELIVERYNOTE	E8h	TIM Container Lieferschein (“delivery note“) → 2.6.21	3.. 23	(TLV-Obj.)	X	X
TIM_CONTAINER_ TRAINING	E9h	TIM Container Training (“training“) → 2.6.21	6.. 21	(TLV-Obj.)		X

Die je Befehl notwendigen oder erlaubten Datenfelder sowie deren Reihenfolge sind jeweils in den einzelnen Erläuterungen im Kapitel → 2.6 spezifiziert.

2.5 LENGTH (Länge)

Folgende Kodierung für die Länge der TLV-Objekte wird verwendet:

Die Länge des Nutzdatenfeldes wird in einem Byte direkt kodiert (00h..7Fh).

In der aktuellen Version der TIM-Spezifikation werden keine Felder mit Längen größer als 127 (7Fh) verwendet. Das hier verwendete BER-TLV ist identisch zum „SIMPLE-TLV“.

2.6 VALUE (Nutzdaten)

Dieses Kapitel definiert die Dateninhalte, die für die Nutzdaten der TLV-Objekte zu verwenden sind. Die auf dem TIM intern zur Speicherung genutzten Formate dürfen von diesen

[10] Container sind zusammengesetzte Datenobjekte. Sie können die TLV-Objekte D8h, D9h, DAh, DBh, DCh und DEh enthalten. Siehe → 2.2.

abweichen und werden durch den Hersteller der TIM-Applikation dokumentiert. Diese internen Formate sind an der TIM-Schnittstelle nicht sichtbar.

Die TLV-Objekte mit dem Präfix „TIM“ werden in Befehlen und Antworten auf der TIM-Schnittstelle verwendet.

2.6.1 TIM Signatur: TIM_SIGNATURE – 9Eh

Die Signatur wird als Folge von zwei 192/256-Bit-Binärzahlen (MSB first) übertragen (insgesamt also 384/512 Bit = 48/64 Byte), siehe Fußnote 1. Beiden Zahlen werden direkt aufeinander folgend in einem einzigen TLV-Objekt übertragen. Eine Unterdrückung führender Null-Bytes findet nicht statt.

Die Signatur wird auf dem TIM für Buchungen bzw. Tagesabschlüsse entsprechend der jeweiligen Hashvorschrift generiert (→ 7.1 bzw. → 7.2).

Beispiel ECDSA-192

T	L	V	Inhalt
9Eh	30h	4Ah 07h 1Ch 49h 3Fh 4Fh BDh 3Eh 8Dh 0Dh FBh 1Ah D4h 98h D6h DBh DEh 71h BEh E2h 92h 5Eh 51h FAh B1h 31h 89h B9h 92h 4Eh 96h 1Fh 2Dh 7Ch 18h 3Ch 20h 83h B0h 65h 33h 99h EDh 6Dh D2h 8Ch F0h D6h	Signatur

Beispiel ECDSA-256

T	L	V	Inhalt
9Eh	40h	4Ah 07h 1Ch 49h 3Fh 4Fh BDh 3Eh 8Dh 0Dh FBh 1Ah D4h 98h D6h DBh DEh 71h BEh E2h 92h 5Eh 51h FAh B1h 31h 89h B9h 92h 4Eh 96h 1Fh 2Dh 7Ch 18h 3Ch 20h 83h B0h 65h 33h 99h EDh 6Dh D2h 8Ch F0h D6h 01h 43h 3Eh 22h 1Ch 5Dh 11h 71h 89h D6h 3Ch A4h 7Fh 22h 4Dh 1Bh	Signatur

2.6.2 TIM Lebenszyklus: TIM_LIFECYCLE – C0h

Der Lebenszyklus gibt den gegenwärtigen Zustand des TIM an und ist auf dem TIM gespeichert. Der Lebenszyklus wird als TLV-Objekt mit der Nutzdatenlänge ein Byte zurückgegeben. Die Kodierung des Lebenszyklus und die Lebenzyklus-Übergänge sind unter → 5 dargelegt.

Beispiel

T	L	V	Inhalt
C0h	01h	03h	TIM ist aktiviert

2.6.3 TIM Seriennummer: TIM_SERIAL_NO – C1h

Die Seriennummer des TIM ist eine eindeutige Identifikationsnummer, die durch den Hersteller der zugrunde liegenden Smart Card vergeben wird. Das Format dieser Seriennummer wird durch den Smart Card Hersteller vorgegeben und kann hier nicht spezifiziert werden.

2.6.4 TIM Version: TIM_VERSION – C2h

Die Versionsnummer der TIM-Applikation wird im Format

A.V.R.M

mit einem Buchstaben und drei durch Punkte getrennte Ziffernfolgen (jeweils max. zwei Ziffern) kodiert. Die Länge des TLV-Objekts TIM Version beträgt 7..10 Byte. Die Elemente der Versionsnummer haben die in Tabelle 2-3 beschriebenen Bedeutungen.

Tabelle 2-3: Definition der TIM Versionsnummer

	Bedeutung	Beschreibung
A	Anwendung	'T' für Testversion, 'V' für Version im Wirkbetrieb
V	Version	Version der TIM Spezifikation
R	Release	kompatible Erweiterungen der Spezifikation
M	Maintenance	ausschließlich Fehlerkorrekturen

Ein TIM entspricht in der jeweiligen Ausprägung der kryptographischen Algorithmen genau einer Version & Release (V.R) der Spezifikation.

Beispiel

T	L	V	Inhalt
C2h	07h	54h 2Eh 31h 2Eh 31h 2Eh 30h	"T.1.1.0"
C2h	07h	56h 2Eh 32h 2Eh 31h 2Eh 30h	"V.2.1.0"

2.6.5 TIM Transport-PIN: TIM_TRANSPORT_PIN – C3h

Die Transport-PIN besteht aus genau 6 Zeichen, die bei der Personalisierung des TIM eingetragen werden. Die Transport-PIN wird als ASCII-Ziffern (30h..39h) kodiert. Zur Aktivierung des TIM (→ 3.5.4) wird die Transport-PIN direkt aufeinander folgend ohne Unterdrückung führender Nullen übertragen.

Beispiel

T	L	V	Inhalt
C3h	06h	30h 31h 32h 33h 34h 35h	'0' '1' '2' '3' '4' '5'

2.6.6 TIM Steuerpflichtigen-ID: TIM_TP_ID – C4h

Die Steuerpflichtigen-ID dient der steuerlichen Zuordnung der mit der Kasse signierten Daten und des TIM. Genutzt werden kann dazu die Wirtschaft Identifikations Nummer (WID), soweit vorhanden. Alternativ kann die Umsatzsteuer-Ident-Nummer (USt-IdNr) verwendet werden. Die Steuerpflichtigen-ID bildet zusammen mit der laufenden Nummer des TIM (→ 2.6.7) ein eindeutiges Identifikationsmerkmal. Gegebenenfalls wird die Finanzverwaltung hier Konkretisierungen vornehmen.

Während der Personalisierung des TIM auf den Steuerpflichtigen wird die Steuerpflichtigen-ID auf dem TIM eingetragen. Sie ist mit 1..32 ASCII-Zeichen im Wertebereich 21h..7Eh definiert. Leerzeichen sind nicht erlaubt. Nach einem Befehl TRANSACTION (alle relevanten Varianten) oder REPORT wird die Steuerpflichtigen-ID – C4h und die laufende Nummer des TIM – C5h dem zu signierenden Datensatz hinzugefügt und in der jeweiligen Antwort zurückgegeben.

Beispiel

T	L	V	Inhalt
C4h	0Ch	44h 45h 30h 31h 32h 33h 34h 35h 36h 37h 38h 39h	Steuerpflichtigen-ID: "DE0123456789"

2.6.7 TIM lfd. Nummer: TIM_TP_ID_NO – C5h

Die laufende Nummer des TIM (je Steuerpflichtigen-ID) wird mit 1-4 Byte binär ohne Vorzeichen auf dem TIM gespeichert und übertragen. Führende Null-Bytes werden weggelassen.

Beispiel

T	L	V	Inhalt
C5h	02h	01h A0h	Lfd. Nummer des TIM: 416

2.6.8 TIM Bediener ID: TIM_OPERATOR – C6h

Die Identifikation des Bedieners wird mit 1..16 ASCII Zeichen im Wertebereich 21h..7Eh übertragen. Die übergebenen Daten werden durch die TIM-Applikation im Hinblick auf den Wertebereich überprüft. Sofern das Nutzdatenfeld Zeichen außerhalb des Wertebereichs 21h..7Eh enthält, wird die Fehlermeldung 98 04h TIM_ERROR_INVALID_CHARACTER zurückgegeben.

Die Bediener-ID muss vor der Übergabe an das TIM von der Kasse entsprechend der Zeichenersetzung aufbereitet werden (→ 6.2). Der Wertebereich wird dabei weiter eingeschränkt.

Beispiel

T	L	V	Inhalt
C6h	10h	6Ch 69h 73h 65h 6Ch 6Fh 74h 74h 65h 23h 62h 65h 72h 73h 63h 68h	'l' 'i' 's' 'e' 'l' 'o' 't' 't' 'e' '#' 'b' 'e' 'r' 's' 'c' 'h' nach Zeichenersetzung (Original: "Liselotte Überschwang" wird zu liselotte#berschwang und dann auf 16 Zeichen gekürzt)

2.6.9 TIM Hashwert der Buchungspositionen: TIM_HASH_TRANSACTION_ITEMS – C7h

Der Hashwert der Buchungspositionen wird als 20/32 Byte Binärwert, siehe Fußnote 1, übertragen (MSB first). Führende Nullbytes werden nicht unterdrückt.

Der Hashwert der Buchungspositionen ist das Ergebnis des verwendeten Profils (→ 9). Je nach Profil wird der Hashwert der Buchungspositionen entsprechend der jeweiligen Hashvorschrift des Profils errechnet.

Beispiel SHA-1 (20 Byte)

T	L	V	Inhalt
C7h	14h	5Bh 3Ch 07h E5h A9h 4Eh 34h 9Bh 2Dh BDh EEh C4h 4Bh 3Eh B9h FDh 62h 98h F0h 33h	Hashwert der Buchungspositionen

Beispiel SHA-256 (32 Byte)

T	L	V	Inhalt
C7h	20h	D3h 2Bh 56h 8Ch D1h B9h 6Dh 45h 9Eh 72h 91h EBh F4h B2h 5Dh 00h 7Fh 27h 5Ch 9Fh 13h 14h 9Bh EEh B7h 82h FAh C0h 71h 66h 13h F8h	Hashwert der Buchungspositionen

2.6.10 TIM Hashwert der Tagesabschluss-Positionen: TIM_HASH_REPORT_ITEMS – D4h

Der Hashwert der Tagesabschluss-Positionen wird als 20/32 Byte Binärwert, siehe Fußnote 1, übertragen (MSB first). Führende Nullbytes werden nicht unterdrückt.

Der Hashwert der Tagesabschluss-Positionen ist das Ergebnis des verwendeten Profils. Je nach Profil wird der Hashwert der Tagesabschluss-Positionen genutzt und entsprechend der jeweiligen Hashvorschrift des Profils errechnet.

Beispiel SHA-1 (20 Byte)

T	L	V	Inhalt
D4h	14h	5Bh 3Ch 07h E5h A9h 4Eh 34h 9Bh 2Dh BDh EEh C4h 4Bh 3Eh B9h FDh 62h 98h F0h 33h	Hashwert der Tagesabschluss-Positionen

Beispiel SHA-256 (32 Byte)

T	L	V	Inhalt
D4h	20h	D3h 2Bh 56h 8Ch D1h B9h 6Dh 45h 9Eh 72h 91h EBh F4h B2h 5Dh 00h 7Fh 27h 5Ch 9Fh 13h 14h 9Bh EEh B7h 82h FAh C0h 71h 66h 13h F8h	Hashwert der Tagesabschluss-Positionen

2.6.11 TIM Währungscode: TIM_CURRENCY – C8h

Der Währungscode wird auf dem TIM während der Personalisierung eingetragen. Bei jeder Buchung wird der Währungscode an das TIM übertragen. Das TIM vergleicht beide Codes und gibt bei negativem Ergebnis den Fehler 98 13h TIM_ERROR_CURRENCY zurück (→ 4).

Der Währungscode wird der ISO 4217 folgend festgelegt, wobei hier die numerische Kodierung genutzt wird. Der Code wird als 2 Byte Binärwert (MSB first) übertragen – führende Nullen werden **nicht** unterdrückt. Für Euro ist der Währungscode 978 bzw. 03 D2h.

Beispiel

T	L	V	Inhalt
C8h	02h	03h D2h	Währungscode Euro: 978

2.6.12 TIM Länderkennzeichen: TIM_COUNTRY_CODE – D5h

Das Länderkennzeichen wird auf dem TIM während der Personalisierung eingetragen. Es dient der Unterscheidung verschiedener Länder bei gleichem Währungscode.

Anmerkung: Das Länderkennzeichen ist optional. Über dessen Eintrag entscheidet die Personalisierungsstelle.

Das Länderkennzeichen wird gemäß ISO 3166 festgelegt, wobei die numerische Kodierung genutzt wird. Der Code wird als 2 Byte Binärwert (MSB first) übertragen – führende Nullen werden **nicht** unterdrückt.

Für Deutschland ist der Ländercode beispielsweise 276 bzw. 01 14h.

Beispiel

T	L	V	Inhalt
D5h	02h	01h 14h	Ländercode Deutschland: 276

2.6.13 TIM Merker exkl. Steuer, Training, Umsatzüberlauf, Umsatzsteuerwechsel: TIM_VAT_ADDON – C9h, TIM_TRAINING – CAh, TIM_DELIVERYNOTE – D7h, TIM_TURNOVER_OVERFLOW – DDh, TIM_TURNOVER_VAT_CHANGED – DEh

Merker (zum Beispiel Überlauf) werden als TL-Objekte ohne VALUE (Nutzdaten) kodiert. Das Längenfeld LENGTH enthält die Länge 00h.

Ein gesetzter Merker wird ausschließlich durch das Vorhandensein des TL-Objekts angezeigt. Nicht gesetzte Merker werden nicht übertragen.

Beispiel

T	L	V	Inhalt
C9h	00h	-	Merker exkl. Steuer gesetzt
CAh	00h	-	Merker Training gesetzt
D7h	00h	-	Merker Lieferschein gesetzt
DDh	00h	-	Merker Umsatzüberlauf gesetzt
DEh	00h	-	Merker Umsatzsteuersatzwechsel gesetzt

2.6.14 TIM Sequenznummern: TIM_SEQ_NO_TRANSACTION – CBh, TIM_SEQ_NO_REPORT – CCh TIM_SEQ_NO_TRANSACTION_FIRST – D2h TIM_SEQ_NO_TRANSACTION_LAST – D3h

Die Sequenznummern für Buchungen und Tagesabschlüsse werden als vorzeichenloser 32 Bit Binärwert (MSB first) vom TIM gesendet. Die Länge des TLV-Objekts ist variabel, 1..4 Bytes. Führende Null-Bytes werden unterdrückt.

Auf dem TIM sind zwei Sequenznummernzähler festgelegt: einer für signierte Buchungen (→ 3.4) und einer für signierte Tagesabschlüsse (→ 3.5.1). Die Sequenznummernzähler werden nur bei Vergabe einer Signatur inkrementiert.

In der Antwort eines Tagesabschlusses werden die beiden Sequenznummern TIM_SEQ_NO_TRANSACTION_FIRST und TIM_SEQ_NO_TRANSACTION_LAST zurückgegeben. Diese geben die Sequenznummer der ersten und letzten Buchung der Umsatzperiode an.

Beispiel

T	L	V	Inhalt
CBh	02h	04h D2h	Sequenznummer Buchung: 1234
CCh	01h	0Fh	Sequenznummer Tagesabschluss: 15
D2h	03h	01h E2h 40h	Sequenznummer der ersten Buchung der Umsatzperiode: 123456
D3h	04h	07h 5Bh CDh 15h	Sequenznummer der letzten Buchung der Umsatzperiode: 123456789

2.6.15 TIM Datum:

TIM_DATE – CDh
TIM_MONTH_START – D0h
TIM_MONTH_END – D1h

Datumsangaben werden in den Formaten

YYYYMMDD oder

YYYYMM

als unsigned BCD übertragen. YYYY bezeichnet die vierstellige Jahreszahl, MM die zweistellige Monatsnummer und DD das zweistellige Tagesdatum.

Das verwendete Format wird anhand der Länge der Nutzdaten (4 bzw. 3 Byte) unterschieden. Das Datum TIM_DATE mit einer Länge von 3 Byte wird bei den GET DATA Befehlen (→ 3.2.2 und → 3.2.3) verwendet.

Die TLV-Objekte TIM_MONTH_START und TIM_MONTH_END definieren den Beginn und das Ende einer Umsatzperiode im Format YYYYMM. Die Länge beträgt ebenfalls 3 Byte.

Alle anderen Befehle nutzen das Datum mit der Länge 4 Byte.

Datumsangaben werden von der TIM-Applikation auf das korrekte Format und den Wertebereich (max. Gültigkeitsdauer des TIM) überprüft.

Beispiel

T	L	V	Inhalt
D0h	03h	20h 09h 02h	'2' '0' '0' '9', '0' '2'
CDh	04h	20h 09h 02h 24h	'2' '0' '0' '9', '0' '2', '2' '4'

2.6.16 TIM Uhrzeit:

TIM_TIME – CEh

Uhrzeitangaben werden im Format

hhmm

im 24- Stunden- Format als unsigned BCD übertragen.

Mit hh wird zweistellig die Stunde und mm die Minute angegeben. Die Länge des TLV-Objekts ist 2 Byte.
Der Wertebereich umfasst 00 00h bis 23 59h.

Beispiel

T	L	V	Inhalt
CEh	02h	23h 09h	'2' '3' '0' '9'

2.6.17 TIM Monat: TIM_MONTH – CFh

Liste von Monaten; jeder Monat wird als Offset zum ersten Monat, in den gebucht werden kann, übertragen. Ein Monat wird als vorzeichenloser 8 Bit Binärwert übertragen. Die Liste kann auch leer sein; in diesem Fall werden lediglich das Tag (CFh) und die Länge null (00h) übertragen.

Die exakte Bedeutung einer Monatsliste ist bei den Kommandos beschrieben (siehe auch → 3.2.3 und 3.2.6).

Beispiel

T	L	V	Inhalt
CDh	03h	20h 08h 01h	Datum "2008","01" → 01/2008 ist der erste Monat, in den gebucht werden kann
CFh	04h	00h 0Ah 0Dh 0Eh	Monat 0, 10, 13, 14 Offset zum ersten Monat der Gültigkeit → Liste umfasst die Monate 01/2008, 11/2008, 02/2009 und 03/2009

Mit dem TAG CDh wird der erste Gültigkeitsmonat des TIM angezeigt.

2.6.18 TIM Umsatz, Negativumsatz, Umsatzsteuer und Umsatz Agenturgeschäft: TIM_TURNOVER – D8h, TIM_TURNOVER_NEGATIVE – D9h, TIM_TURNOVER_VAT – DAh TIM_TURNOVER_THIRDPARTY –D6h

Umsätze und Umsatzsteuer werden im Datentyp signed BCD übertragen (siehe → 2.3.4). Führende Null-Bytes müssen unterdrückt werden.

Alle Werte werden auf die kleinste Währungseinheit (hier: Euro-Cent) normiert, so dass kein Dezimalzeichen verwendet wird.

Umsätze und Umsatzsteuern mit dem Wert Null dürfen nicht übertragen werden. In diesen Fällen ist das jeweilige TLV-Objekt wegzulassen. Das TLV-Objekt Umsatz gibt den resultierenden Gesamtumsatz der Buchung je Umsatzsteuerklasse an. Umsätze aus Agenturgeschäft müssen im Gesamtumsatz und ggfs. dem Gesamtnegativumsatz der Umsatzsteuerklasse enthalten sein. Negativumsätze reduzieren den Umsatz und den zugehörigen Betrag der Umsatzsteuer. Negativumsätze werden im TLV-Objekt Negativumsatz ausgewiesen und als positive Zahl übertragen.

Der Umsatz einer Buchung darf auch negativ sein. Sofern der Umsatz negativ ist, muss ein Negativumsatz an das TIM übergeben werden, der größer oder gleich dem absoluten Betrag des Umsatzes ist. Größere Negativumsätze ergeben sich dann, wenn der Umsatz aus positiven und negativen Buchungspositionen resultieren.“

Umsätze und Negativumsätze bezeichnen die umsatzsteuerbezogenen Gesamtsummen einer Buchung. Diese sind nicht mit den in Profilen festgelegten Preisen einzelner Buchungspositionen zu verwechseln.

Der Umsatz Agenturgeschäft muss die Summe aller Buchungspositionen Agenturgeschäft eines Umsatzsteuersatzes enthalten. Diese Summe wird TIM-intern als Bruttoumsatz im Container Agenturumsatz summiert.

Umsatz, Negativumsatz, Umsatzsteuer und Umsatz Agenturgeschäft werden bei einer Buchungsanfrage immer in einem Container (→ 2.6.21) übertragen.

Beispiele für gültige und ungültige Kodierungen (Währungseinheit: Euro-Cent):

T	L	V	Inhalt
D8h	02h	12h 3Ch	Umsatz: 1,23 €
D8h	03h	01h 23h 4Dh	Umsatz: -12,34 €
DAh	01h	1Ch	Umsatzsteuer: 0,01 €
D9h	04h	01h 00h 00h 0Ch	Negativumsatz: 1000,00 €
D8h	06h	00h 00h 00h 00h 12h 3Ch	**ungültig**, führende Null-Bytes nicht unterdrückt
D8h	03h	34h 56h 70h	**ungültiges** Vorzeichen
D9h	01h	0Dh	**ungültiges** Vorzeichen für Null
D6h	02h	12 3Dh	Umsatz Agenturgeschäft: -1,23 €

2.6.19 TIM Umsatzsteuersatz: TIM_TURNOVER_VAT_RATE – DBh

Umsatzsteuersätze werden im Datentyp unsigned BCD mit 2 oder 4 gültigen Stellen übertragen (siehe → 2.3.3).

Alle Werte werden auf die kleinste Einheit 0,01 % normiert. Somit wird kein Dezimalzeichen verwendet.

Ein führendes Null-Byte muss unterdrückt werden. Ein Umsatzsteuersatz von 0% muss übertragen werden.

Beispiele

Beispiele für gültige und ungültige Kodierungen:

T	L	V	Inhalt
DBh	02h	19h 00h	Umsatzsteuersatz: 19%
DBh	02h	05h 50h	Umsatzsteuersatz: 5,5%
DBh	02h	07h 00h	Umsatzsteuersatz: 7%
DBh	01h	00h	0%, umsatzsteuerfrei
DBh	02h	00h 10h	**ungültig**, führendes Null-Byte nicht unterdrückt

2.6.20 TIM Zähler der Buchungen: TIM_TURNOVER_COUNTER – DCh

Die jeweiligen Zähler der Buchungen für Agentur-, Lieferschein- und Trainingsspeicher werden auf dem TIM verwaltet und als vorzeichenloser 32 Bit Binärwert (MSB first) zurückgegeben (siehe → 2.3.3).

Führende Null-Bytes werden unterdrückt. Das TLV-Objekt besitzt eine variable Länge von 1..4 Byte.

Beispiele

T	L	V	Inhalt
DCh	02h	0Bh 00h	Zähler der Buchungen: 2816
DCh	03h	01h FFh 01h	Zähler der Buchungen: 130817

2.6.21 TIM Container 1…6 und Container für Agenturgeschäft, Lieferschein und Training: TIM_CONTAINER_VAT_1…6 – E1h…E6h, TIM_CONTAINER_THIRDPARTY – E7h, TIM_CONTAINER_DELIVERYNOTE – E8h, TIM_CONTAINER_TRAINING – E9h

Die Container 1..6 und die Container Agenturgeschäft (→Glossar, 8.2.2), Lieferschein (→Glossar, 8.2.3) und Training (→Glossar, 8.2.4) mit den Tags E1h..E9h sind zusammengesetzte Datenobjekte (→ 2.2.).

Sie können folgende TLV-Objekte enthalten:

- Umsatz, Negativumsatz, Umsatzsteuer (Tags D8h..DAh→ 2.6.18),
- Umsatz Agenturgeschäft (Tag D6h) bei Buchungsanfrage
- Umsatzsteuersatz (Tag DBh → 2.6.19)
- Zähler der Buchungen (Tag DCh → 2.6.20) und
- Merker Umsatzüberlauf und Änderung Umsatzsteuersatz (Tags DDh, DEh → 2.6.12).

Durch die Tags für Container 1..6, Container für Agenturgeschäft, Lieferschein und Training werden die Speicher auf dem TIM angegeben, in denen die Umsätze aktualisiert werden sollen (→ 8.2) Je nach Umsatzsteuerklasse muss der entsprechende Container 1..6 verwendet werden. Die Zuordnung ist im Abschnitt → 6.1.1 definiert.

Für die Übertragungsrichtung zum TIM sind lediglich die Datenobjekte D6h, D8h, D9h, DAh und DBh erlaubt. In der Richtung vom TIM können Antworten des REPORT zusätzlich die Datenobjekte DCh..DEh enthalten (→ 2.6.12, 2.6.20).

Die Container E7h und E8h enthalten die vom TIM verwalteten Bruttosummen für Transaktionen aus Umsätzen Agenturgeschäft bzw. Lieferschein.

Wenn in einem Container Umsatz und Negativumsatz den Wert Null haben, wird dieser Container nicht übertragen.

Die Gültigkeit der übergebenen Werte wird durch das TIM überprüft. Diese Prüfung umfasst die korrekte Kodierung sowie bei Negativumsätzen den Vergleich mit dem Umsatz – ist der Umsatz negativ, so muss der Negativumsatz größer oder gleich dem Absolutbetrag des

Umsatzes sein.
Beispiel: Umsatz = -100 € → Negativumsatz muss größer/gleich 100 € sein

Beispiele

Container 1 mit Standard Umsatzsteuersatz, Umsatz = +11,99 €, (Negativumsatz = 0 € entfällt), Umsatzsteuer = +1,91 €, Umsatzsteuersatz = 19,00 %

T_C	L_C	V_C												
		T_{P1}	L_{P1}	V_{P1}			T_{P2}	L_{P2}	V_{P2}		T_{P3}	L_{P3}	V_{P3}	
E1h	0Dh	D8h	03h	01h	19h	9Ch	DAh	02h	19h	1Ch	DBh	02h	19h	00h

Produktrücknahme -11,99 €, Einkauf +11,99 €, beides 7% USt
Container 2 mit ermäßigtem Umsatzsteuersatz 7%, (Umsatz = +11,99 € - 11,99 € = 0 € entfällt), Negativumsatz = +11,99 € , (Umsatzsteuer = -0,78 € + 0,78 € = 0 € entfällt), Umsatzsteuersatz = 7,00 %

TC	LC	VC								
		TP 1	LP 1	VP1			TP 2	LP 2	VP2	
E2h	09h	D9h	03h	01h	19h	9Ch	DBh	02h	07h	00h

3 Befehle

Die in Tabelle 3-1 beschriebenen Befehle sind an der TIM-Schnittstelle verfügbar:

Tabelle 3-1: Befehle der TIM-Applikation

Befehl	Kodierung CLA INS P1 P2	Optionen
SELECT FILE	00h A4h 0xh 0yh	x, y Kodierung gemäß ISO 7816-4 → 3.1
GET DATA	00h CAh 01h yyh	yy = F0 – TIM-Status yy = F1 – TIM-Status, extended yy = F2 – Booked Months yy = F3 – Hash Length yy = F4 – Cryptograhic Algorithms yy = F5 – Memory Status → 3.2
READ CERTIFICATE	00h B0h xxh yyh	ISO 7816-4 Befehl READ BINARY xx, yy Kodierung gemäß ISO Short File-Ids werden nicht unterstützt → 3.3
TRANSACTION	80h 40h xxh 00h	xx = 00 – TRANSACTION xx = 01 – TR Data xx = 02 – TR Tax Payer xx = 03 – TR Time Stamp → 3.4
REPORT	80h 42h xxh 00h	xx = 01 – Signed xx = 02 – Unsigned xx = 03 – Span xx = 04 – TIM Activate xx = 05 – TIM Deactivate → 3.5
GET LATEST RESPONSE	80h C0h 00h 00h	→ 3.6
VERIFY SIGNATURE	80h 44h 00h 00h	→ 3.7
HASH	00h 2Ah 90h 80h bzw. 10h 2Ah 90h 80h	ISO 7816-8 Befehl PSO_H → 3.8

Die Befehle GET DATA und REPORT bieten Optionen, die dem Befehlsnamen angehängt werden, z.B. „GET DATA TIM Status“. Nachfolgend werden die Befehle näher erläutert. Bei jedem Befehl wird ein Result Code zurückgegeben(→ 4).

Anmerkung: Die Kodierungen in diesem Kapitel geben sinnvolle Werte für LE an - nicht die nach ISO 7816 ausschließlich gültigen.

3.1 SELECT FILE

Der SELECT FILE Befehl wählt die TIM-Applikation oder eine der zugehörigen Dateien aus. Es handelt sich um das Standard ISO 7816-4 Kommando. Die möglichen Optionen für P1 und P2 sind in der ISO 7816-4 definiert.

3.1.1 Auswahl der TIM-Applikation

Die TIM-Applikation wird als „default selected“ Anwendung auf der Smart Card installiert. Daher stehen alle Befehle der TIM-Applikation nach dem Anlegen der Versorgungsspannung – oder einem RESET – unmittelbar zur Verfügung.
Eine explizite Auswahl der Applikation ist nicht notwendig – aber möglich. Damit wird die Kompatibilität zu den Vorgängerkarten sichergestellt.

Die Auswahl der TIM-Applikation kann über die registrierte Application-ID (AID) erfolgen. Die AID besteht für den ECDSA-192-Modus aus dem Registered Identifier (RID)[11]: **D2h 76h 00h 01h 48h** plus der Propritary application Identifier eXtension (PIX): **'T' 'I' 'M' (**54h 49h 4Dh**)**.
Für ECDSA-256-Modus wird die RID D2h 76h 00h 01h 72h plus PIX **'T' 'I' 'M'** verwendet. Die Variante der TIM-Applikation wird bei der Personalisierung des TIM festgelegt. Es ist jeweils nur die personalisierte Variante (192 Bit **oder** 256 Bit) selektierbar.

Die Länge der übergebenen Daten wird im LC Feld angegeben. P2 = 0Ch unterdrückt die Rückgabe von Werten, somit muss die Länge der erwarteten Antwort (LE) nicht angegeben werden, darf aber. Die vollständige Kodierung für den Befehl ist daher:

Befehl

CLA	INS	P1	P2
00h	A4h	04h	0Ch

Datenfeld für ECDSA-192-Modus

LC	Data	LE
08h	D2h 76h 00h 01h 48h 54h 49h 4Dh	--

Data

AID (hier: D2h 76h 00h 01h 48h 54h 49h 4Dh)

Datenfeld für ECDSA-256-Modus

LC	Data	LE
08h	D2h 76h 00h 01h 72h 54h 49h 4Dh	--

Data

AID (D2h 76h 00h 01h 72h 54h 49h 4Dh)

Antwort

SW1 / SW2	
67 00h	LC ungültig
6A 82h	Datei / Anwendung nicht gefunden.
6A 86h	P1 / P2 ungültig
90 00h	Kein Fehler

[11] Siehe: http://www.kartenbezogene-identifier.de/de/rapi/rid-liste.html

3.1.2 Auswahl einer Datei

Die Auswahl einer Datei erfolgt über die File-ID (FID). Die Länge der übergebenen Daten wird im LC Feld angegeben. P2 = 0Ch unterdrückt die Rückgabe von Werten, somit muss die Länge der erwarteten Antwort (LE) nicht angegeben werden.

Das folgende Beispiel zeigt die Selektion der Zertifikats-Datei. Das Zertifikat ist auf dem TIM in der Datei **EF_CERT** mit der File-ID **11h 10h** gespeichert. Die vollständige Kodierung für den Befehl zur Selektion der Datei EF_CERT ist daher:

Befehl

CLA	INS	P1	P2
00h	A4h	00h	0Ch

LC	Data	LE
02h	11h 10h	--

Data

File-ID (hier: EF_CERT = 11h 10h)

Antwort

SW1 / SW2	
67 00h	LC ungültig
6A 82h	Datei / Anwendung nicht gefunden.
6A 86h	P1 / P2 ungültig
90 00h	Kein Fehler

3.2 GET DATA

Der GET DATA Befehl liest Informationen über die TIM-Applikation. Dieser Befehl erweitert den ISO 7816 Befehl gleichen Namens.

Das Datenfeld dieses Befehles ist leer. Lediglich die Länge der erwarteten Antwort ist im LE Feld zu kodieren (00h → alle Daten).

Der Befehl bietet drei Varianten, die anhand der Kodierung von P2 unterschieden werden. In den nachfolgenden Abschnitten werden die Varianten detailliert erläutert.

Befehl

CLA	INS	P1	P2
00h	CAh	01h	siehe Tabelle 3-2

LC	Data	LE
--	--	00h

Tabelle 3-2: GET DATA Parameter P2

P2	Bedeutung
F0h	GET DATA TIM Status → 3.2.1
F1h	GET DATA TIM Status, extended → 3.2.2
F2h	GET DATA TIM Booked Months → 3.2.3
F3h	GET DATA Hash Length → 3.2.4
F4h	GET DATA Cryptographic Algorithms→3.2.5
F5h	GET DATA Memory Status → 3.2.6

Antwort

Siehe nachfolgende Abschnitte → 3.2.1 – 3.2.4

3.2.1 GET DATA TIM Status

Auf den Befehl GET DATA mit P2 = F0h sendet das TIM eine kurze Statusinformation.

Befehl

CLA	INS	P1	P2
00h	CAh	01h	F0h

LC	Data	LE
--	--	00h

Antwort

Folgende Datenobjekte werden TLV-kodiert zurückgegeben:

Tag	Length (Byte)	Value
C0h	1	Lebenszyklus des TIM → 2.6.2

SW1 / SW2	
67 00h	LC ungültig
6A 86h	P1 / P2 ungültig
90 00h	Kein Fehler

3.2.2 GET DATA TIM Status extended (TIM Status, erweitert)

Auf den Befehl GET DATA mit P2 = F1h sendet das TIM erweiterte Statusinformationen.

Befehl

CLA	INS	P1	P2
00h	CAh	01h	F1h

LC	Data	LE
--	--	00h

Antwort

Die in Tabelle 3-3 aufgelisteten Datenobjekte werden TLV-kodiert zurückgegeben.

Tabelle 3-3: TLV Antwort mit erweitertem TIM-Status

Tag	Length (Byte)	Value
C0h	1	Lebenszyklus des TIM → 2.6.2
C2h	7..10	TIM-Version → 2.6.4
C4h	1..32	Steuerpflichtigen-ID → 2.6.6
C5h	1..4	lfd. Nummer des TIM → 2.6.7
C1h	*	Seriennummer des TIM → 2.6.3
C8h	2	Währungscode → 2.6.10
D5h	2	Länderkennzeichen → 2.6.12, sofern konfiguriert
CDh	3	Datum (des letzten buchbaren Monats) → 2.6.15
CBh	1..4	Sequenznummer für Buchungen (aktuell) 2.6.14
CCh	1..4	Sequenznummer für Tagesabschlüsse (aktuell) → 2.6.14
CDh	4	Datum der Personalisierung (LC ≥ 02) → 2.6.15
CDh	4	Datum der Aktivierung (LC ≥ 03) → 2.6.15
CDh	4	Datum der Deaktivierung (LC ≥ 04) → 2.6.15
02h	1	Art der Deaktivierung (LC ≥ 04) → Tabelle 3-4

* Die Länge der Serienummer ist von der verwendeten Smart Card abhängig und wird durch den Hersteller spezifiziert.

SW1 / SW2	
67 00h	LC ungültig
6A 86h	P1 / P2 ungültig
90 00h	Kein Fehler

Die Felder „Datum der Personalisierung“, „Datum der Aktivierung“, „Datum der Deaktivierung“ und „Art der Deaktivierung“ werden nur im angegebenen Lebenszyklus der Karte zurückgegeben.

Das Feld „Art der Deaktivierung“ gibt an, wodurch das TIM deaktiviert wurde, siehe Tabelle 3-4:

Tabelle 3-4: Art der Deaktivierung

Code	Art der Deaktivierung
00h	Deaktivierung durch REPORT TIM Deactivate
01h	Speicherfehler
02h	Falscheingabe der PIN
03h	Interner Fehler
04h … 7Fh	Reserviert für TIM Spezifikation.
80h … FFh	Verwendbar durch TIM Lieferant.

3.2.3 GET DATA TIM Booked Months (Liste der Umsatzmonate)

Auf den Befehl GET DATA mit P2 = F2h sendet das TIM eine Liste der Monate, in denen bisher Umsätze gebucht wurden.

Befehl

CLA	INS	P1	P2
00h	CAh	01h	F2h

LC	Data	LE
--	--	00h

Antwort

Die in Tabelle 3-5 aufgelisteten Datenobjekte werden TLV-kodiert zurückgegeben.

Tabelle 3-5: TLV Antwort mit Liste der Umsatzmonate

TAG	Length (Byte)	Value
CDh	3	Zeitpunkt des ersten Monats, in den gebucht werden kann → 2.6.15
CFh	0..121	Liste der Monate mit Umsatz, ein Monat mit Umsatz wird als binärer Offset zum ersten Monat, in den gebucht werden kann (→ CDh) übertragen → 2.6.17

Die Monate, in denen bisher Umsatz gebucht wurde, werden als Offset zum dem Monat übertragen, in den die erste Buchung möglich ist. Die Anzahl der bereits gebuchten Monate ist daher aus der Länge des Nutzdatenfeldes ersichtlich.

Ein Beispiel dieser Antwort findet sich unter → 2.6.17.

SW1 / SW2	
67 00h	LC ungültig
6A 86h	P1 / P2 ungültig
90 00h	Kein Fehler

3.2.4 GET DATA Hash Length

Auf den Befehl GET DATA mit P2 = F3h sendet das TIM die Länge der unterstützten Hash-Werte für TRANSACTION und REPORT Befehle.

Befehl

CLA	INS	P1	P2
00h	CAh	01h	F3h

LC	Data	LE
--	--	00h

Antwort

Die in Tabelle 3-6 aufgelisteten Datenobjekte werden TLV-kodiert zurückgegeben:

Tabelle 3-6: TLV Antwort mit Länge des Hashwertes

TAG	Length (Byte)	Value
02h	1	Länge des Hash-Wertes in Byte

SW1 / SW2	
67 00h	LC ungültig
6A 86h	P1 / P2 ungültig
90 00h	Kein Fehler

3.2.5 GET DATA Cryptographic Algorithms

Auf den Befehl GET DATA mit P2 = F4h sendet das TIM die OIDs der verwendeten kryptographischen Algorithmen.

Befehl

CLA	INS	P1	P2
00h	CAh	01h	F4h

LC	Data	LE
--	--	00h

Antwort

Die in Tabelle 3-7 aufgelisteten Datenobjekte werden – in der angegebenen Reihenfolge – zurückgegeben.

Tabelle 3-7: TLV Antwort mit Länge des OID

TAG	Length (Byte)	Value
06h	l_{OID}	OID des Signatur-Algorithmus (ECDSA mit SHA-1 / ECDSA mit SHA-256)
06h	l_{OID}	OID der zugrundeliegenden Kurve (192 / 256 bit)
06h	l_{OID}	OID des Hash-Algorithmus für Buchungspositionen (SHA-1 / SHA-256)

Die OIDs, siehe Tabelle 3-8, werden alle mit dem gleichen Tag 06h übergeben (gemäß ASN.1-Tag für OIDs); Die Bedeutung ergibt sich aus der Position bzw. dem Wert. Die Länge der Signatur kann aus dem zweiten Antworttag anhand der OID der Kurve ermittelt werden. Die Länge des zu übergebenen Buchungspositions-Hashwertes ergibt sich aus der OID des Hash-Algorithmus des dritten Tags. Tabelle 3-8 zeigt in der ersten Zeile jeweils die OID in ASN.1 Punktnotation und in der zweiten Zeile die OID in ASN.1 DER-Kodierung.

SW1 / SW2	
67 00h	LC ungültig
6A 86h	P1 / P2 ungültig
90 00h	Kein Fehler

Tabelle 3-8: Vom TIM verwendete Object-Identifier

OID	Bedeutung
1.2.840.10045.4.1 06 07 2A8648CE3D0401	Signatur-Algorithmus: ECDSA mit SHA-1
1.2.840.10045.4.3.2 06 08 2A8648CE3D040302	Signatur-Algorithmus: ECDSA mit SHA-256
1.2.840.10045.3.1.1 06 08 2A8648CE3D030101	ECC-Kurve: NIST 192bit (random)
1.2.840.10045.3.1.7 06 08 2A8648CE3D030107	ECC-Kurve: NIST 256bit (random)
1.3.14.3.2.26 06 05 2B0E03021A	Hash-Algorithmus: SHA-1
2.16.840.1.101.3.4.2.1 06 09 608648016503040201	Hash-Algorithmus: SHA-256

3.2.6 GET DATA Memory Status

Auf den Befehl GET DATA mit P2 = F5h sendet das TIM den Status des internen Speichers.

Dies kann nach einem Speicherfehler zur genaueren Analyse verwendet werden.
Eine Auswertung der gespeicherten Daten über den Befehl REPORT ist weiterhin möglich!

Befehl

CLA	INS	P1	P2
00h	CAh	01h	F5h

LC	Data	LE
--	--	00h

Antwort

Die in Tabelle 3-9 aufgelisteten Datenobjekte werden TLV-kodiert zurückgegeben.

Bei einem Fehler im Konfigurationsspeicher kann auch das Monatsdatum (CDh) falsch sein; die Liste der Monate mit Speicherfehler ist dennoch korrekt!

Tabelle 3-9: TLV Antwort mit Status des Speichers

TAG	Length (Byte)	Value
01h	1	00h: **kein** Fehler im Konfigurationsspeicher FFh: **Fehler** im Konfigurationsspeicher
CDh	3	Zeitpunkt des ersten Monats, in den gebucht werden kann → 2.6.15
CFh	0..121	Liste der Monate mit Speicherfehler. Ein Monat mit Speicherfehler wird als binärer Offset zum ersten Monat, in den gebucht werden kann (→ CDh) übertragen → 2.6.17

SW1 / SW2	
67 00h	LC ungültig
6A 86h	P1 / P2 ungültig
90 00h	Kein Fehler

3.3 READ CERTIFICATE

Mit dem Befehl READ CERTIFICATE wird das auf dem TIM gespeicherte Zertifikat ausgelesen. Das Zertifikat beinhaltet Angaben zum Steuerpflichtigen sowie den öffentlichen Schlüssel des TIM und wird im Format X.509v3 gespeichert. Die Angaben im Zertifikat der TIM sind eine Teilmenge von Tabelle 8-1.

Der Befehl READ CERTIFICATE entspricht dem ISO 7816-4 Befehl READ BINARY. Die Kodierung der Parameter P1 und P2 entspricht damit der ISO Norm.

Das Zertifikat ist auf dem TIM im Elementary File EF_CERT mit der File-ID 1110h abgelegt. Die zu lesende Datei ist über den SELECT FILE Befehl auszuwählen (Auswahl des Zertifikats siehe → 3.1.2). Short File-IDs (SFID) werden nicht unterstützt.

Die ISO 7816-3 definiert Antworten mit maximal 254 Byte Informationslänge. Je nach Konfiguration kann das TIM längere Antworten zurückgeben. Aufgrund der Beschränkung muss das Zertifikat in mehreren Schritten gelesen werden. Im ersten Schritt wird ein Teil der Daten gelesen. In weiteren Schritten kann unter Angabe des Offset der Rest der Daten gelesen werden.

Das Datenfeld des Befehls ist leer. Die Länge der zu lesenden Daten ist im LE Feld zu kodieren (00h → maximale Antwortlänge). Zur Vereinfachung der Berechnungen kann hier zum Beispiel mit einer Länge von 128 Byte (80h) gearbeitet werden.

Ein Beispiel zum Auslesen des Zertifikats findet sich unter → 10.1.4.

Befehl

CLA	INS	P1	P2
00h	B0h	xx	yy

LC	Data	LE
--	--	*

* Länge der angeforderten Daten

Parameter P1 / P2

Kodierung P1 (xx) High-Byte (Offset)
Kodierung P2 (yy) Low-Byte (Offset)

Der Offset kann maximal 32767 (dezimal) / 7FFFh (hex) betragen.

Antwort

Daten
Angeforderte Daten

SW1 / SW2	
xx xxh	siehe Fehlermeldungen (→ 4) und ISO 7816-4
90 00h	Kein Fehler

3.4 TRANSACTION

Der Befehl TRANSACTION übergibt die Daten einer Buchung oder eines frei wählbaren Datenblocks an das TIM.

Beim Signieren beliebiger Daten in freier Wahl des aufrufenden Systems muss im INSIKA-Umfeld der zu signierende Datensatz immer mindestens mit der kartenintern generierten Sequenznummer verbunden werden. Nur so ist der Nachweis der Vollständigkeit der Datenaufzeichnung gegeben. Zur Verifikation des signierten Datensatzes sind alle von der TIM-

Applikation in Abhängigkeit vom verwendeten Transaktionsbefehl ergänzten Datenelemente erforderlich.

Die Länge der übergebenen Daten wird im LC Feld angegeben (mit * gekennzeichnet). Die Länge der erwarteten Antwort ist im LE Feld zu kodieren (00h → alle Daten).

Befehl

CLA	INS	P1	P2
80h	40h	00h, 01h / 02h / 03h	00h

LC	Data	LE
*	Daten (siehe → 3.4.1 – 3.4.2	00h

* Länge der übergebenen Daten

Parameter P1

P1	Bedeutung
00h	TRANSACTION
01h	TR Data
02h	TR Tax Payer
03h	TR Time Stamp

3.4.1 TRANSACTION (Buchung)

Das TIM plausibilisiert bei Buchungen die übergebenen Daten[12]. Bei positivem Ergebnis generiert das TIM eine eindeutige Sequenznummer, aktualisiert die internen Summenspeicher, bereitet die Daten entsprechend der Hashvorschrift TRANSACTION (→7.1.1) auf, signiert den Datensatz und gibt die Signatur zurück. Bei negativem Ergebnis wird ein Fehlercode (→ 4) zurückgegeben. Vor einer Buchung muss der Hashwert der Buchungspositionen berechnet werden. Die Vorschriften dazu finden sich in der Definition des entsprechenden Profils (vgl. → 1.4 und → 9).

Befehl

CLA	INS	P1	P2
80h	40h	00h	00h

LC	Data	LE
*	Buchungsdaten → Tabelle 3-10	00h

* Länge der übergebenen Buchungsdaten

Data

Die Buchungsdaten enthalten die TLV-Objekte gemäß Tabelle 3-10.

[12] Das TIM führt eine semantische, syntaktische und inhaltliche Plausibilisierung der übergebenen Datenstruktuen bzw. Umsatzdaten durch.

Tabelle 3-10: Buchungs – Anfrage

Tag	Length (Byte)	Value	ggf. nicht übertragen[13]	signaturrelevant[14]
CDh	4	Datum → 2.6.15		X
CEh	2	Uhrzeit → 2.6.16		X
C6h	1..16	Bediener-ID → 2.6.8		X
C7h	20/32	Hashwert der Buchungspositionen → 2.6.9		X
C8h	2	Währungscode → 2.6.11	X[15]	
C9h	0	Merker „Exklusiv Steuer“ → 2.6.13	X	X
CAh	0	Merker „Trainings Modus“ → 2.6.13	X	X
D7h	0	Merker „Lieferschein“ → 2.6.13	X	X
E1h	6..28	Container 1 → 2.6.21	X	
D8h	1..6	Umsatz → 2.6.18		X
D9h	1..6	Negativumsatz → 2.6.18	X	
DAh	1..6	Umsatzsteuer → 2.6.18	X	
DBh	1..2	Umsatzsteuersatz → 2.6.19		X
D6h	1..6	Umsatz Agenturgeschäft → 2.6.18	X	X
		…	X	
E6h	6..28	Container 6 → 2.6.21	X	
D8h	1..6	Umsatz → 2.6.18		X
D9h	1..6	Negativumsatz → 2.6.18	X	
DAh	1..6	Umsatzsteuer → 2.6.18	X	
DBh	1..2	Umsatzsteuersatz → 2.6.19		X
D6h	1..6	Umsatz Agenturgeschäft → 2.6.18	X	X

Bemerkung: Alle Umsätze bzw. Werte ungleich Null sind zu übertragen; bei Nullumsätzen bzw. nicht gesetztem Merker wird das Datenobjekt weggelassen.

Trainingsumsätze werden durch den Merker „Trainings Modus“ (Tag CAh → 2.6.12) gekennzeichnet.

[13] Nullumsätze und nicht gesetzte Merker werden nicht übertragen.

[14] Datenobjekt geht direkt in die Signatur ein

[15] Bei Buchungsanfragen mit Umsätzen ungleich Null muss C8h -Währungscode übertragen werden.

Wenn der Merker exkl. Steuer (→ 2.6.12) nicht übertragen wurde, werden die Umsätze und Negativumsätze als Bruttowerte behandelt. Wird der Merker exkl. Steuer übertragen, werden die Umsätze und Negativumsätze als Nettowerte behandelt.

Antwort bei positiver Plausibilisierung

Bei positiver Plausibilisierung der Buchung[16] werden die in der Personalisierung auf dem TIM eingetragene Steuerpflichtigen-ID, die lfd. Nummer des TIM und die auf dem TIM generierte Sequenznummer und Signatur zurückgegeben.

Tag	Length (Byte)	Value
C4h	1..32	Steuerpflichtigen-ID → 2.6.6
C5h	1..4	lfd. Nummer des TIM → 2.6.7
CBh	1..4	Sequenznummer der Buchung → 2.6.14
9Eh	48/64	Signatur der Buchung → 2.6.21

SW1 / SW2	
90 00h	Kein Fehler

Antwort bei negativer Plausibilisierung oder Fehlern

Bei negativer Plausibilisierung werden je nach Grund verschiedene Result-Codes zurückgegeben:

SW1 / SW2	
xx xxh	siehe Fehlermeldungen (→ 4) und ISO 7816-4
62 00h	Warnung: Der Befehl konnte nicht abgeschlossen werden.
67 00h	LC ungültig
6A 86h	P1 / P2 ungültig
98 13h	TIM_ERROR_CURRENCY → 4
98 21h	TIM_ERROR_TAX_VERIFICATION_FAILED → 4
98 22h	TIM_ERROR_NEGATIVE_TURNOVER → 4

Umsatz-Plausibilisierung des TIM

Es werden folgende Bedingungen geprüft:

1. Die Plausibilität von Umsatz, Umsatzsteuer und Umsatzsteuersatz wird durch das TIM überprüft. Sofern der Merker exkl. Steuer nicht übertragen wurde, wird der Umsatz als Bruttowert betrachtet, andernfalls als Nettowert. Schlägt diese Plausibilisierung fehl, wird der Result-Code 98 21h TIM_ERROR_TAX_VERIFICATION_FAILED zurückgegeben.
2. Sofern der Umsatz negativ ist, muss ein Negativumsatz an das TIM übergeben werden, der größer oder gleich dem absoluten Betrag des Umsatzes ist. Der Umsatz und

[16] Das TIM führt eine semantische, syntaktische und inhaltliche Plausibilisierung der übergebenen Datenstruktuen bzw. Umsatzdaten durch.

der zugehörige Betrag der Umsatzsteuer werden vor der Übertragung an das TIM um den jeweiligen Anteil des Negativumsatzes reduziert. (Bsp: 100 Euro Einnahme - 10 Euro Warenrücknahme = 90 Euro Umsatz und 10 Euro Negativumsatz) Negativumsätze werden als positive Zahl übertragen. Schlägt die Plausibilisierung der Negativumsätze fehl, wird der Result-Code 98 22h TIM_ERROR_NEGATIVE_TURNOVER zurückgegeben.

3. Ein positiver Agenturumsatz wird gegen den Positivumsatz validiert, ein negativer Agenturumsatz gegen den Negativumsatz. In beiden Fällen muss der Agenturumsatz betragsmäßig kleiner oder gleich dem Vergleichsumsatz sein. Ist er größer, wird der Result-Code 98 23h TIM_ERROR_THIRD_PARTY zurückgegeben.
4. Buchungsanfragen die nur aus dem Umsatzsteuersatz Ex/DBh (x=1..6) bestehen (Nullumsatz) werden vom TIM zurückgewiesen.
   Nullumsätze in einer USt-Klasse dürfen nicht an das TIM übergeben werden!

Nur wenn alle Plausibilisierungen für die übergebenen Container erfolgreich durchgeführt werden konnten, wird die Buchung signiert und die Umsatzspeicher des TIM aktualisiert (siehe dazu → 8.2).

Wird eine Buchungsanfrage ohne Umsatz gestellt, d.h. keiner der Container 1..6 wird übergeben, da alle Buchungspositionen den Umsatzwert NULL enthalten oder in den Buchungspositionen kein Umsatz enthalten ist, wird die Signatur über die restlichen übergebenen Datenelemente gebildet. Ein Umsatz-Container mit lediglich dem Feld Umsatzsteuersatz wäre durchaus gültig!

> **Hinweis:** In der Version T.1.1.0 des TIM wurde dies bisher mit dem Fehler TIM_ERROR_DATA_MISSING beantwortet.
> Eine Buchung ohne Umsatz (Container 1..6 sowie Negativumsatz leer, also nicht übertragen) ist sinnvoll, z.B. um die Abgabe von Waren ohne Berechnung zu dokumentieren.

3.4.2 TR Data

Bei Nutzung des Befehls TR Data zur Signatur eines frei wählbaren Datenblocks muss der Hashwert über den zu signierenden Datenblock übergeben werden. Das TIM prüft die korrekte Länge des übergebenen Hashwerts, generiert die Transaktions-Sequenznummer, bereitet die Daten entsprechend der Hashvorschrift (→Tabelle 7-2) auf, signiert den Datensatz und gibt die Sequenznummer und Signatur zurück. Bei negativem Ergebnis wird ein Fehlercode (→ 4) zurückgegeben.

Befehl

CLA	INS	P1	P2
80h	40h	01h	00h

LC	Data	LE
*	Transaktionsdaten→ Tabelle 3-11	00h

* Länge der übergebenen Transaktionsdaten

Data

Die Transaktionsdaten enthalten TLV-Objekte gemäß Tabelle 3-11.

Tabelle 3-11: TR Data– Anfrage

Tag	Length (Byte)	Value
C7h	20/32	Hashwert der zu signierenden Daten

Antwort bei positiver Plausibilisierung

Tag	Length (Byte)	Value
CBh	1..4	Sequenznummer der Transaktion→ 2.6.14
9Eh	48	Signatur der Transaktion → 2.6.21

Antwort bei negativer Plausibilisierung

Bei negativer Plausibilisierung werden je nach Grund verschiedene Result-Codes zurückgegeben:

SW1 / SW2	
xx xxh	siehe Fehlermeldungen (→ 4) und ISO 7816-4
67 00h	LC ungültig
6A 86h	P1 / P2 ungültig

3.4.3 TR _Tax Payer

Der Befehl TR TaxPayer entspricht im Wesentlichen dem Befehl TR Data, siehe 3.4.2 in Bezug auf die TR Tax Payer-Anfrage. Die Antwort enthält jedoch zusätzlich die TAGs C4h und C5h, die entsprechend Hashvorschrift Tabelle 7-2 vom TIM in die Signatur einbezogen werden. Bei negativem Ergebnis wird ein Fehlercode (→ 4) zurückgegeben.

Befehl

CLA	INS	P1	P2
80h	40h	02h	00h

LC	Data	LE
*	Transaktionsdaten → Tabelle 3-12	00h

* Länge des übergebenen Hashwertes

Data

Die Transaktionsdaten enthalten TLV-Objekte gemäß Tabelle 3-12.

Tabelle 3-12: TR Tax Payer– Anfrage

Tag	Length (Byte)	Value
C7h	20/32	Hashwert der zu signierenden Daten

Antwort bei positiver Plausibilisierung

Tag	Length (Byte)	Value
C4h	1..32	Steuerpflichtigen-ID → 2.6.6
C5h	1..4	lfd. Nummer des TIM → 2.6.7
CBh	1..4	Sequenznummer der Buchung → 2.6.14
9Eh	48	Signatur der Buchung → 2.6.21

Antwort bei negativer Plausibilisierung

Siehe 3.4.2.

3.4.4 TR Time Stamp

Der Befehl TR Time Stamp entspricht im Wesentlichen dem Befehl TR Data, siehe 3.4.2. Die Anfrage TR Time Stamp muss allerdings zusätzlich zum Hashwert über den Datenblock die TAGs für Datum und Uhrzeit enthalten. Die Antwort ist mit der Antwort in 0 identisch. Bei negativem Ergebnis wird ein Fehlercode (→ 4) zurückgegeben.

Befehl

CLA	INS	P1	P2
80h	40h	03h	00h

LC	Data	LE
*	Transaktionsdaten→ Tabelle 3-13	00h

* Länge des übergebenen Hashwertes

Data

Die Transaktionsdaten enthalten TLV-Objekte gemäßTabelle 3-13.

Tabelle 3-13: TR Time Stamp– Anfrage

Tag	Length (Byte)	Value
CDh	4	Datum → 2.6.15
CEh	2	Uhrzeit → 2.6.16
C7h	20/32	Hashwert der zu signierenden Daten

Antwort bei positiver Plausibilisierung

Tag	Length (Byte)	Value
C4h	1..32	Steuerpflichtigen-ID → 2.6.6
C5h	1..4	lfd. Nummer des TIM → 2.6.7
CBh	1..4	Sequenznummer der Buchung → 2.6.14
9Eh	48	Signatur der Buchung → 2.6.21

Antwort bei negativer Plausibilisierung

Siehe 3.4.2.

3.5 REPORT (Tagesabschluss)

Der Befehl REPORT gibt die Summenspeicher des TIM aus. Der Befehl bietet fünf Varianten, die anhand der Kodierung des Parameters P1 unterschieden werden. In den nachfolgenden Abschnitten werden die Varianten detailliert erläutert.

Der Inhalt des Datenfelds ist von der Befehlsvariante abhängig. Die Länge der erwarteten Antwort ist im LE Feld zu kodieren (00h → alle Daten).

Befehl

CLA	INS	P1	P2
80h	42h	01h / 02h / 03h / 04h / 05h	00h / 01h / 02h

LC	Data	LE
*	Daten (siehe → 3.5.1 - 3.5.5)	00h

* Länge der übergebenen Daten

Parameter P1

P1	Bedeutung
01h	REPORT Signed
02h	REPORT Unsigned
03h	REPORT Span
04h	REPORT TIM Activate
05h	REPORT TIM Deactivate

Antwort

Die Antwort ist für jeden dieser Report-Befehle identisch und daher nur einmal dargestellt.

Tabelle 3-14: Antwort REPORT

Tag	Length (Byte)	Value	ggf. nicht über-tragen[17]
C0h	1	Lebenszyklus des TIM → 2.6.2	
C4h	1..32	Steuerpflichtigen-ID → 2.6.6	
C5h	1..4	lfd. Nummer des TIM → 2.6.7	
CCh	1..4	Sequenznummer des Tagesabschluss → 2.6.14	
D2h	1..4	Sequenznummer der ersten Buchung der Umsatzperiode → 2.6.14	
D3h	1..4	Sequenznummer der letzten Buchung der Umsatzperiode → 2.6.14	
E1h	6..34	Container 1 → 2.6.21	X
D8h	1..11	Umsatz → 2.6.18	
D9h	1..11	Negativumsatz → 2.6.18	X
DBh	1..2	Umsatzsteuersatz → 2.6.19	
DDh	0	Merker Umsatzüberlauf → 2.6.13	X
DEh	0	Merker Änderung Umsatzsteuersatz → 2.6.13	X
		…	X
E6h	6..34	Container 6 → 2.6.21	X
D8h	1..11	Umsatz → 2.6.18	
D9h	1..11	Negativumsatz → 2.6.18	X
DBh	1..2	Umsatzsteuersatz → 2.6.19	
DDh	0	Merker Umsatzüberlauf → 2.6.13	X
DEh	0	Merker Änderung Umsatzsteuersatz → 2.6.13	X
E7h	6..23	Container Agenturgeschäft → 2.6.21	X
D8h	1..11	Umsatz → 2.6.18	
DCh	1..4	Zähler der Buchungen → 2.6.20	
DDh	0	Merker Umsatzüberlauf → 2.6.13	X
E8h	6..23	Container Lieferschein → 2.6.21	X
D8h	1..11	Umsatz → 2.6.18	

[17] Nicht bebuchte Container und nicht gesetzte Merker werden nicht übertragen.

Tag	Length (Byte)	Value	ggf. nicht übertragen[17]
DCh	1.4	Zähler der Buchungen → 2.6.20	
DDh	0	Merker Umsatzüberlauf → 2.6.13	X
E9h	6..21	Container Training → 2.6.21	X
D8h	1..11	Umsatz → 2.6.18	
DCh	1..4	Zähler der Buchungen → 2.6.20	
DDh	0	Merker Umsatzüberlauf → 2.6.13	X
9Eh	48/64	Signatur → 2.6.1	X[18]

Für jeden Container ist der zurückgegebene Umsatzsteuersatz jeweils der Umsatzsteuersatz des zuletzt ausgelesenen Monats.

SW1 / SW2	
xx xxh	siehe Fehlermeldungen (→ 4) und ISO 7816-4
67 00h	LC ungültig
6A 80h	ungültige Parameter im Datenfeld
98 D1h	Antwort erfordert “extended Length”
90 00h	Kein Fehler

Anmerkungen zu den Fehlercodes:

Die Antwort auf den Befehl REPORT kann die Länge von 256 Byte überschreiten. In diesem Fall gibt das TIM lediglich die Warnung TIM_WARNING_ANSWER_LENGTH (98 D1h) – aber keine REPORT Daten – zurück. In diesem Fall muss der REPORT Befehl als Extended Length APDU wiederholt werden.

3.5.1 REPORT Signed (Tagesabschluss mit Signatur)

Dieser Befehl erstellt einen signierten Tagesabschluss. Hierzu werden die Umsatzsummen über alle gebuchten Umsätze gebildet und zurückgegeben. Auf dem TIM werden dazu die Summen über alle gebuchten Monate gebildet. Optional kann ein Hashwert über zusätzliche Tagesabschlussdaten übergeben und damit in die Signatur einbezogen werden.

Es wird eine Signatur gemäß Abbildungsvorschrift (→ 7.2) erstellt und die Sequenznummer des Tagesabschlusses inkrementiert. Die Antwort enthält das Datenobjekt Signatur (9Eh).

Das Datenfeld dieses Befehls enthält Datum und Uhrzeit entsprechend → Tabelle 3-15. Die Länge der erwarteten Antwort ist im LE Feld zu kodieren (00h → alle Daten).

[18] Die Signatur wird nur bei den Befehlen REPORT Signed, TIM Activate und TIM Deactivate zurückgegeben

Befehl

CLA	INS	P1	P2
80h	42h	01h	00h

LC	Data	LE
*	Datum/Uhrzeit/Hashwert → Tabelle 3-15	00h

* Länge der übergebenen Daten

Data

Datum und Uhrzeit und (optionaler) Hashwert werden wie folgt angegeben:

Tabelle 3-15: Datum/Uhrzeit der Report-Anfrage

Tag	Length (Byte)	Value	ggf. nicht übertragen
CDh	4	Datum → 2.6.15	
CEh	2	Uhrzeit → 2.6.16	
D4h	20/32	Hashwert der Tagesabschluss-Positionen	X

Antwort

Siehe → 3.5

3.5.2 REPORT Unsigned (Tagesabschluss ohne Signatur)

Dieser Befehl erstellt einen Tagesabschluss ohne Signatur. Hierzu werden die Umsatzsummen über alle gebuchten Umsätze gebildet und zurückgegeben. Auf dem TIM werden dazu die Summen über alle gebuchten Monate gebildet.

Es wird keine Signatur gebildet. Die Sequenznummer des Tagesabschlusses bleibt unverändert. In der Antwort wird kein Datenobjekt Signatur (9Eh) übertragen.

Das Datenfeld dieses Befehls enthält Datum und Uhrzeit entsprechend → Tabelle 3-16. Die Länge der erwarteten Antwort ist im LE Feld zu kodieren (00h → alle Daten).

Befehl

CLA	INS	P1	P2
80h	42h	02h	00h / 01h / 02h

LC	Data	LE
0Ah	Datum/Uhrzeit → Tabelle 3-16	00h

Parameter P2

P2	Bedeutung
00h	Speicherfehler werden gemeldet (98 E2h).
01h	Speicherfehler werden ignoriert; fehlerbehaftete Monatsspeicher werden aufsummiert.
02h	Speicherfehler werden ignoriert; fehlerbehaftete Monatsspeicher werden **nicht** aufsummiert.

Data

Datum und Uhrzeit werden wie folgt angegeben:

Tabelle 3-16: Datum/Uhrzeit der Report-Anfrage

Tag	Length (Byte)	Value
CDh	4	Datum → 2.6.15
CEh	2	Uhrzeit → 2.6.16

Antwort

Siehe → 3.5

3.5.3 REPORT Span („Von-Bis“ Summe)

Dieser Befehl ermittelt die Umsatzsummen über einen Datumsbereich.

Im Datenfeld dieses Befehles werden Startmonat und Endmonat für die Summation spezifiziert. Die Länge der erwarteten Antwort ist im LE Feld zu kodieren (00h bedeutet alle Daten). Die Umsatzdaten werden nicht signiert und die Sequenznummer des Tagesabschlusses bleibt unverändert. In der Antwort wird das Datenobjekt Signatur (9Eh) nicht übertragen.

Befehl

CLA	INS	P1	P2
80h	42h	03h	00h / 01h / 02h

LC	Data	LE
14h	Umsatzperiode → Tabelle 3-17	00h

Parameter P2

P2	Bedeutung
00h	Speicherfehler werden gemeldet (98 E2h).
01h	Speicherfehler werden ignoriert; fehlerbehaftete Monatsspeicher werden aufsummiert.
02h	Speicherfehler werden ignoriert; fehlerbehaftete Monatsspeicher werden **nicht** aufsummiert.

Data

Die Umsatzperiode wird wie folgt angegeben:

Tabelle 3-17: Umsatzperiode

Tag	Length (Byte)	Value
CDh	4	Datum → 2.6.15
CEh	2	Uhrzeit → 2.6.16
D0h	3	Erster Monat der Umsatzperiode → 2.6.15
D1h	3	Letzter Monat der Umsatzperiode → 2.6.15

Antwort

Siehe → 3.5

3.5.4 REPORT TIM Activate (TIM Aktivierung)

Dieser Befehl aktiviert das TIM. Damit wird der Übergang des TIM in LC 03 ausgelöst, siehe 5.

Hierzu werden die Umsatzsummen über alle Monate gebildet und inklusive einer Sequenznummer und Signatur zurückgegeben. Im Datenfeld dieses Befehls müssen die TIM Transport-PIN, das Datum und die Uhrzeit übergeben werden. Die Länge der erwarteten Antwort ist im LE Feld zu kodieren (00h → alle Daten).

Befehl

CLA	INS	P1	P2
80h	42h	04h	00h

LC	Data	LE
12h	**Aktivierungsdaten →** Tabelle 3-18	00h

Data

Tabelle 3-18: Aktivierungsdaten

Tag	Length (Byte)	Value
CDh	4	Datum → 2.6.15
CEh	2	Uhrzeit → 2.6.16
C3h	6	Transport PIN → 2.6.5

Antwort

Siehe → 3.5

3.5.5 REPORT TIM Deactivate (TIM Deaktivierung)

Dieser Befehl deaktiviert das TIM dauerhaft! Eine erneute Aktivierung ist nicht möglich (siehe Lebenszyklus des TIM → 5).

Hierzu werden die Umsatzsummen über alle Monate gebildet und inklusive einer Sequenznummer und Signatur zurückgegeben.

Die Länge der erwarteten Antwort ist im LE Feld zu kodieren (00h → alle Daten).

Befehl

CLA	INS	P1	P2
80h	42h	05h	00h

LC	Data	LE
0Ah	Deaktivierungsdaten → Tabelle 3-19	00h

Data

Tabelle 3-19: Deaktivierungsdaten

Tag	Length (Byte)	Value
CDh	4	Datum → 2.6.15
CEh	2	Uhrzeit → 2.6.16

Antwort

Siehe → 3.5

3.6 GET LATEST RESPONSE

Mit dem Befehl GET LATEST RESPONSE kann das Ergebnis des letzten Befehls TRANSACTION oder REPORT nochmals abgerufen werden. Die Ergebnisse eines TRANSACTION- oder REPORT-Befehls werden getrennt voneinander nichtflüchtig gespeichert; die Ergebnisse können auch nach einem Spannungsausfall oder Reset der Karte ausgelesen werden. Die Nutzung dieses Befehls ist optional.

Wurde wegen einer Kommunikationsstörung zwischen Karte und System die Antwort auf den Befehl TRANSACTION bzw. REPORT nicht ordnungsgemäß empfangen, kann das System die Antwort per GET LATEST RESPONSE erneut abrufen.

Wird dabei nicht die erwartete Sequenznummer geliefert, ist der vorherige TRANSACTION- bzw. REPORT-Befehl nicht korrekt ausgeführt worden. In diesem Fall ist der entsprechende Befehl TRANSACTION bzw. REPORT erneut auszuführen.

Der Parameter P1 wählt den Speicherbereich aus:

P1 = 00h Ergebnis der letzten TRANSACTION

P1 = 01h Ergebnis des letzten REPORT

Befehl

CLA	INS	P1	P2
80h	C0h	00h/01h	00h

LC	Data	LE
--	--	00h

Antwort

siehe 3.4, falls GET LATEST RESPONSE erfolgreich durchgeführt wurde.

Falls GET LATEST RESPONSE nicht erfolgreich ist, wird folgende Fehlermeldung generiert:

SW1 / SW2	
98 E2h	Prüfsummenfehler im LATEST REPONSE Speicher. LATEST RESPONSE wurde gelöscht.
65 00h	Ausführungsfehler, Zustand des nichtflüchtigen Speichers möglicherweise verändert, es kann keine Information geliefert werden

3.7 VERIFY SIGNATURE

Mit dem Befehl VERIFY SIGNATURE lassen sich für alle Varianten des Befehls TRANSACTION erhaltenen Signaturen überprüfen. Die Nutzung ist für alle Varianten dieses Befehls optional.

Die Daten für die Signaturverifikation werden nach der Übergabe entsprechend der Hashvorschriften TRANSACTION (→ 7.1) durch das TIM sortiert und dann mit Hilfe des öffentlichen Schlüssels verifiziert. Die Signatur eines Tagesabschlusses (REPORT) kann mit diesem Befehl nicht verifiziert werden.

Die Länge der übergebenen Daten wird im LC Feld angegeben (unten mit * gekennzeichnet). Die Länge der erwarteten Antwort ist im LE Feld zu kodieren (00h → alle Daten).

Befehl

CLA	INS	P1	P2
80h	44h	00h, 01h / 02h / 03h	00h

LC	Data	LE
*	Daten für die Signaturverifikation → Variantenabhängig	00h

* Länge der übergebenen Daten

Parameter P1

P1	Bedeutung
00h	TRANSACTION
01h	TR Data
02h	TR Tax Payer
03h	TR Time Stamp

3.7.1 TRANSACTION (Buchung)

Befehl

CLA	INS	P1	P2
80h	44h	00h	00h

LC	Data	LE
*	Buchungsdaten → Tabelle 3-20	00h

* Länge der übergebenen Buchungsdaten

Data

Für die Verifikation der erhaltenen Signatur werden die ursprünglichen Daten der Buchung, die erhaltene Sequenznummer und die erhaltene Signatur übergeben. Es müssen TLV-Objekte gemäß Tabelle 3-20 übergeben werden.

Tabelle 3-20: Daten für die Signaturverifikation TRANSACTION (Buchung)

Tag	Length (Byte)	Value	ggf. nicht übertragen[19]
CDh	4	Datum → 2.6.15	
CEh	2	Uhrzeit → 2.6.16	
C6h	1..16	Bediener-ID → 2.6.8	
C7h	20/32	Hashwert der Positionsdaten → 2.6.9	
C9h	0	Merker „Exklusiv Steuer“ → 2.6.13	X
CAh	0	Merker „Trainings Modus“ → 2.6.13	X
D7h	0	Merker „Lieferschein“ → 2.6.13	X
CBh	1..4	Sequenznummer der Buchung → 2.6.14	
E1h	6..28	Container 1 → 2.6.21	X
D8h	1..6	Umsatz → 2.6.18	X
D9h	1..6	Negativumsatz → 2.6.18	X
DAh	1..6	Umsatzsteuer → 2.6.18	X
DBh	1..2	Umsatzsteuersatz → 2.6.19	
D6h	1..6	Umsatz Agenturgeschäft → 2.6.18	X
		…	X
E6h	6..28	Container 6 → 2.6.21	X
D8h	1..6	Umsatz → 2.6.18	X
D9h	1..6	Negativumsatz → 2.6.18	X
DAh	1..6	Umsatzsteuer → 2.6.18	X
DBh	1..2	Umsatzsteuersatz → 2.6.19	
D6h	1..6	Umsatz Agenturgeschäft → 2.6.18	X
9Eh	48/64	Signatur der Buchung → 2.6.1	

Antwort

Bei positiver Signaturverifikation wird SW1/SW2 = 90 00h zurückgegeben. Schlägt die Signaturverifikation fehl, wird SW1/SW2 = 98 31h zurückgegeben. Weitere Fehlercodes sind möglich.

[19] Nullumsätze und nicht gesetzte Merker werden nicht übertragen.

SW1 / SW2	
xx xxh	siehe Fehlermeldungen (→ 4) und ISO 7816-4
67 00h	LC ungültig
6A 80h	ungültige Parameter im Datenfeld
98 31h	TIM_ERROR _SIGNATURE_INVALID → 4
90 00h	Kein Fehler

3.7.2 TR Data

Befehl

CLA	INS	P1	P2
80h	44h	01h	00h

LC	Data	LE
*	Buchungsdaten → Tabelle 3-21	00h

* Länge der übergebenen Buchungsdaten

Data

Für die Verifikation der erhaltenen Signatur werden der Hashwert des signierten Datensatzes, die erhaltene Sequenznummer und die erhaltene Signatur übergeben. Es müssen TLV-Objekte gemäß Tabelle 3-21 übergeben werden.

Tabelle 3-21: Daten für die Signaturverifikation TR Data

Tag	Length (Byte)	Value	ggf. nicht übertragen
C7h	20/32	Hashwert der zu signierenden Daten	
CBh	1..4	Sequenznummer der Buchung → 2.6.14	
9Eh	48/64	Signatur der Buchung → 2.6.1	

Antwort

Siehe 3.7.1

3.7.3 TR Tax Payer

Befehl

CLA	INS	P1	P2
80h	44h	02h	00h

LC	Data	LE
*	Buchungsdaten → Tabelle 3-22	00h

* Länge der übergebenen Buchungsdaten

Data

Für die Verifikation der erhaltenen Signatur werden der Hashwert des signierten Datensatzes, die erhaltene Sequenznummer und die erhaltene Signatur übergeben. Es müssen TLV-Objekte gemäß Tabelle 3-22 übergeben werden.

Tabelle 3-22: Daten für die Signaturverifikation TR Tax Payer

Tag	Length (Byte)	Value	ggf. nicht übertragen
C7h	20/32	Hashwert der zu signierenden Daten	
CBh	1..4	Sequenznummer der Buchung → 2.6.14	
9Eh	48/64	Signatur der Buchung → 2.6.1	

Hinweis:

Obwohl die übergebenen Daten für die Signaturverifikation mit den Daten aus TR Data identisch sind, bezieht das TIM die intern gespeicherten Informationen mit den Tags C4h und C5h in die Berechnung ein.

Antwort

Siehe 3.7.1

3.7.4 TR Time Stamp

Befehl

CLA	INS	P1	P2
80h	44h	03h	00h

LC	Data	LE
*	Buchungsdaten → Tabelle 3-23	00h

* Länge der übergebenen Buchungsdaten

Data

Für die Verifikation der erhaltenen Signatur werden Datum, Uhrzeit, der Hashwert des signierten Datensatzes, die erhaltene Sequenznummer und die erhaltene Signatur übergeben. Es müssen TLV-Objekte gemäß Tabelle 3-23 übergeben werden.

Tabelle 3-23: Daten für die Signaturverifikation TR Time Stamp

Tag	Length (Byte)	Value	ggf. nicht übertragen
CDh	4	Datum → 2.6.15	X
CEh	2	Uhrzeit → 2.6.16	X
C7h	20/32	Hashwert der zu signierenden Daten	
CBh	1..4	Sequenznummer der Buchung → 2.6.14	
9Eh	48/64	Signatur der Buchung → 2.6.1	

Hinweis:

Das TIM setzt ebenfalls die intern gespeicherten Informationen für die Tags C4h und C5h in die Berechnungen zur Verifikation ein.

Antwort

Siehe 3.7.1

3.8 HASH

Mit dem Befehl HASH lässt sich in Abhängigkeit von der Selektion des Kryptoalgorithmus bei der Antragstellung mit dem TIM T.1.1.0 ein SHA-1 oder TIM V.2.1.0 ein SHA-256 Hashwert berechnen. Die Nutzung dieses Befehls ist optional.

Der Befehl HASH kann beispielsweise genutzt werden, um das TIM zur Berechnung des Hashwerts der Buchungspositionen zu nutzen (→ 2.6.9). Die genauen Vorschriften dazu finden sich in der Definition des jeweiligen Profils (→ 9). Dem TIM werden die Buchungspositionen entsprechend der Hashvorschrift für Buchungspositionen übergeben. Das TIM berechnet den Hashwert und gibt diesen zurück. Das TIM führt keine Überprüfung der Daten durch.

Für eine effiziente Implementierung ist in den meisten Fällen die Verwendung des Befehls HASH nicht optimal. Stattdessen sollte die Berechnung des Hashwerts der Buchungspositionen auf dem Host durchgeführt werden. In der Entwicklung kann der Befehl HASH dabei zur Überprüfung der eigenen SHA-1- bzw. SHA-256-Implementierung genutzt werden.

Der Befehl HASH wird durch den ISO 7816-8 Befehl PSO_HASH (PSO_H) realisiert. Die Kodierung der Parameter P1 und P2 entspricht der ISO Norm.

Die Übergabe der Daten kann in mehreren Schritten geschehen ("Chaining"). Zur Kennzeichnung, dass weitere Datenblöcke folgen, wird das CLA Byte 10h verwendet. Die Übergabe der Daten muss – außer im letzten Schritt (CLA = 00h) – in Vielfachen von 64 Byte (40h) geschehen.

Die Länge der übergebenen Daten wird im LC Feld angegeben. Die Länge der erwarteten Antwort ist im LE Feld zu kodieren (00h → alle Daten oder 14h → Länge eines SHA-1 Hashwertes oder 20h → Länge eines SHA-256 Hashwertes.

Befehl

CLA	INS	P1	P2
00h / 10h	2Ah	90h	80h

LC	Data	LE
*	Daten	00h / 14h bzw. 20h

* Länge der übergebenen Daten

Data

Daten, über die der SHA-1 bzw. SHA-256 Hashwert berechnet werden soll.

Antwort

Daten
Hashwert der Daten (20/32 Byte) / leer (0 Byte)

Der Hashwert wird erst beim letzten Befehl (CLA = 00h) zurückgegeben; bei allen anderen Aufrufen (CLA = 10h) sind die Rückgabedaten leer.

SW1 / SW2	
xx xxh	siehe Fehlermeldungen (→ 4) und ISO 7816-8
90 00h	Kein Fehler

4 Fehlermeldungen (RESULT CODES)

Fehlermeldungen der TIM-Applikation werden über Resultcodes der Befehle übermittelt. Diese Codes werden in den Antwortbytes SW1 und SW2 übertragen (→ ISO 7816-4).

Zusätzlich zu diesen applikationsspezifischen Codes können weitere ISO 7816-4 Fehlercodes auftreten.

Tabelle 4-1 enthält die Fehlercodes, die von der TIM-Applikation zurückgegeben werden.

Tabelle 4-1: Fehlermeldungen des TIM

Kodierung SW1/SW2	Name	Beschreibung
90 00h	NO_ERROR	Befehl erfolgreich ausgeführt. (ISO 7816-4)
98 01h	TIM_ERROR_TLV	Fehler im TLV-Format (Länge, ungültige Tags usw.)
98 02h	TIM_ERROR_VALUE	Das Nutzdatenfeld (Value) mindestens eines TLV-Objekts entspricht nicht der Spezifikation (z.B. Nullumsatz, Vorzeichencodierung nicht korrekt) Bei zusammengesetzten Datenobjekten wird hiermit ein Fehler in den enthaltenen einfachen Datenobjekten signalisiert.
98 03h	TIM_ERROR_ DATA_MISSING	Die übergebenen Daten sind nicht korrekt (Pflicht-Datenobjekt fehlt in übergebenen Daten usw.).
98 04h	TIM_ERROR_ INVALID_CHARACTER	Das Nutzdatenfeld (Value) eines TLV-Objekts enthält mindestens ein ungültiges Zeichen (z.B. in Bediener-ID).
98 11h	TIM_ERROR_ DATE_FORMAT	Das Datum oder die Uhrzeit sind nicht plausibel (z.B. 32.12.2010 oder 24:00 Uhr.
98 12h	TIM_ERROR_ DATE_OUT_OF_RANGE	Das übergebene Datum liegt außerhalb der Gültigkeitsdauer des TIM.
98 13h	TIM_ERROR_ CURRENCY	Der übergebene Währungscode stimmt nicht mit dem auf dem TIM abgespeicherten Code überein.
98 21h	TIM_ERROR_ TAX_VERIFICATION_FAILED	Die Verifikation der übergebenen Werte für Steuer, Umsatz und Umsatzsteuersatz schlug fehl.
98 22h	TIM_ERROR_ NEGATIVE_TURNOVER	Der übergebene Negativumsatz ist nicht plausibel.
98 23h	TIM_ERROR_THIRD_PARTY	Der übergebene Agenturumsatz ist größer als der steuerliche Umsatz.
98 31h	TIM_ERROR_ INVALID_SIGNATURE	Die mit dem Befehl VERIFY SIGNATURE übergebenen Daten (Buchungsdaten, erhaltene Sequenznummer der Buchung und erhaltene Signatur) sind nicht durch das TIM erzeugt worden.
98 41h	TIM_ERROR_ INVALID_LIVECYCLE	Der Befehl ist im gegenwärtigen Lebenszyklus des TIM nicht ausführbar.

Kodierung SW1/SW2	Name	Beschreibung
98 D1h	TIM_WARNING_ ANSWER_LENGTH	Die Länge der Antwort erfordert eine „extended length“ APDU. Daten auf dem TIM wurden nicht verändert. Der Befehl kann wiederholt werden.
98 D2h	TIM_WARNING_INTERNAL	Es ist ein – nicht näher spezifizierter – Fehler bei der Verarbeitung aufgetreten. Daten auf dem TIM wurden nicht verändert. Der Befehl kann wiederholt werden.
98 E0h	TIM_ERROR_OUT_OF_ MEMORY	Speicher auf der Smart Card reicht nicht aus.
98 E1h	TIM_ERROR_ MEMORY_FAILURE	Fehler beim Schreiben in EEPROM, Fehler beim Lesen aus EEPROM . Das TIM wurde zur Sicherheit deaktiviert!
98 E2h	TIM_ERROR_ DATA_CORRUPTED	Die auf dem TIM gespeicherten Daten sind nicht korrekt (Prüfsummenfehler). Das TIM wurde zur Sicherheit deaktiviert!
98 F2h	TIM_ERROR_INTERNAL	Es ist ein – nicht näher spezifizierter – Fehler bei der Verarbeitung aufgetreten. Das TIM wurde zur Sicherheit deaktiviert!
98 FFh	TIM_ERROR_ NOT_SUPPORTED	Funktion / Datenfeld wird derzeit vom TIM nicht unterstützt
65 00h	TIM_ERROR_ EXECUTION_ERROR	Ausführungsfehler, Zustand des nichtflüchtigen Speichers möglicherweise verändert, es kann keine Information geliefert werden

5 Lebenszyklus des TIM

5.1 Kodierung des TIM Lebenszyklus

Tabelle 5-1: Kodierung des Lebenszyklus des TIM

Name	Codierung	Beschreibung
(UNDEFINED)	00h	undefinierter TIM-Lebenszyklus
TIM_INITIALISED	01h	Auf die Smart Card wurde erfolgreich das TIM-Package aufgespielt.
TIM_PERSONALISED	02h	Das TIM ist personalisiert auf den Steuerpflichtigen, die TP_ID, TP_ID_NO, der Währungscode, das Personalisierungsdatum und das Ablaufdatum sind eingetragen.
TIM_ACTIVATED	03h	Das TIM wurde mit Hilfe der Transport-PIN aktiviert. Jetzt können Buchungen signiert, Werte gespeichert und Tagesabschlüsse ausgeben werden.
TIM_DEACTIVATED	04h	Das TIM ist deaktiviert. Es werden keine Buchungen mehr signiert oder gespeichert. Die aufgezeichneten Daten lassen sich weiterhin auslesen.

5.2 Übergänge des TIM Lebenszyklus

Tabelle 5-2: Zustandsübergänge im Lebenszyklus des TIM

Zustand	Übergangsbedingung	Folgezustand
Smart Card ohne TIM Package	Aufspielen des TIM Package	TIM_INITIALISED
TIM_INITIALISED	Personalisierung des TIM durch die ausgebende Stelle	TIM_PERSONALISED
TIM_PERSONALISED	Aktivierung des TIM durch den Steuerpflichtigen mit Hilfe der Transport-PIN	TIM_ACTIVATED
TIM_PERSONALISED	16-fache Fehleingabe der Transport-PIN durch den Steuerpflichtigen	TIM_DEACTIVATED
TIM_ACTIVATED	Deaktivierung des TIM durch den Steuerpflichtigen	TIM_DEACTIVATED
TIM_DEACTIVATED		Keiner

Die Transport-PIN ist als ASCII-Ziffernfolge definiert und besteht aus genau 6 Ziffern. Der Fehlbedienungszähler für die PIN hat den Initialwert 15. Die PIN muss einmalig mit dem Befehl REPORT TIM Activate (80h 42h 04h 00h) verifiziert werden (→ 3.5.4). Das TIM ist dann aktiviert.

Das TIM kann durch den Befehl REPORT TIM Deactivate (80h 42h 05h 00h) dauerhaft deaktiviert werden (→ 3.5.5). Es sind dann keine weiteren Buchungen möglich, der Lesezugriff ist jedoch weiterhin möglich.

Das TIM wird im Lebenszyklus TIM_PERSONALISED an den Steuerpflichtigen ausgeliefert. Sofern die Transport-PIN nicht genutzt werden soll, kann das TIM auch im Lebenszyklus TIM_ACTIVATED ausgeliefert werden.

5.3 Verfügbare Befehle je TIM Lebenszyklus

Tabelle 5-3 gibt eine Übersicht zu den im jeweiligen Lebenszyklus möglichen Befehlen.

Tabelle 5-3: Verfügbare Befehle je TIM Lebenszyklus

TIM Befehl	TIM Lebenszyklus				
	Smart Card ohne TIM Package	TIM_INITIALISED	TIM_PERSONALISED	TIM_ACTIVATED	TIM_DEACTIVATED
SELECT FILE	[§]	X	X	X	X
GET DATA TIM Status	-	X	X	X	X
GET DATA TIM Status extended	-	- *	X	X	X
GET DATA Booked Months	-	- *	X	X	X
GET DATA Hash Length	-	X	X	X	X
GET DATA Cryptographic Algorithms	-	X	X	X	X
GET DATA Memory Status	-	X	X	X	X
TRANSACTION (alle Varianten)	-	- *	- *	X	- *
REPORT signed	-	- *	- *	X	X
REPORT unsigned	-	- *	- *	X	X
REPORT Span	-	- *	- *	X	X
REPORT TIM Activate	-	- *	X	- *	- *
REPORT TIM Deactivate	-	- *	- *	X	- *
GET LATEST RESPONSE	-	- *	- *	X	X
VERIFY SIGNATURE (alle Varianten)	-	- *	- *	X	X
HASH	[§]	X	X	X	X
READ CERTIFICATE	[§]	X	X	X	X

* Es wird der RESULT CODE 98 41h - TIM_ERROR_INVALID_LIVECYCLE zurückgegeben
[§] ISO7816, abhängig vom Smart Card Betriebssystem

6 Definitionen und Festlegungen

6.1 Umsatzsteuerklassen

6.1.1 Definition der Container 1..6

Für umsatzsteuerbezogene Werte sind sechs verschiedene Container definiert, von denen jeder eine Umsatzsteuerklasse abbildet. Die Umsatzsteuerklasse ist hier unabhängig vom jeweils aktuellen Umsatzsteuersatz festgelegt. Die Festlegung der Umsatzsteuersätze ist durch gesetzliche Regelungen vorgeschrieben. Sie wird in der Kasse vorgenommen und ist auf dem TIM nicht vorab gespeichert. Der Umsatzsteuersatz der jeweils letzten Buchung auf einen bestimmten Monat ist jedoch im jeweiligen Container abgelegt.

Tabelle 6-1: Definition der Container 1..6 entsprechend der USt-Klassen

Name	Tag	Bezeichnung Umsatzsteuer-klasse	Bezeichnung und Umsatz-steuersatz in Deutschland (2016)
TIM_CONTAINER_VAT_1	E1h	Standard	Normalsatz: 19%
TIM_CONTAINER_VAT_2	E2h	Ermäßigt 1	Ermäßigter Satz: 7%
TIM_CONTAINER_VAT_3	E3h	Ermäßigt 2	(nicht vorhanden)
TIM_CONTAINER_VAT_4	E4h	umsatzsteuerfrei	0%
TIM_CONTAINER_VAT_5	E5h	Spezial 1	Durchschnittssatz 1: 10,7%
TIM_CONTAINER_VAT_6	E6h	Spezial 2	Durchschnittssatz 2: 5,5%

Mit dieser Einteilung sollte sich die Mehrzahl von Umsatzsteuermodellen abbilden lassen. Innerhalb der Europäischen Union ist dies voraussichtlich problemlos möglich. Zur Einteilung siehe: Amtsblatt der Europäischen Union L347: "Richtlinie 2006/112/EG des Rates vom 28. November 2006 über das gemeinsame Mehrwertsteuersystem" unter:

http://eur-lex.europa.eu/JOHtml.do?uri=OJ%3AL%3A2006%3A347%3ASOM%3ADE%3AHTML

6.2 Zeichenersetzung

Um die Verifikation gedruckter Belege durchführen zu können, müssen vom Befehl-aufrufenden System in den Nutzdaten folgender TLV-Objekte Zeichen ersetzt werden:

- TIM Bediener ID – C6h (→ 2.6.8),
- Texte in Datenfeldern, welche im jeweiligen Profil definiert sind.

Dies betrifft Zeichen, die nicht gedruckt oder nicht aus dem Druckbild eindeutig zurück gewonnen werden können. Die Zeichenersetzung bildet damit die Grundlage für die Überprüfung des Hashwert der Buchungspositionen auf dem Beleg.

Bevor das TLV-Objekt TIM Bediener-ID im Rahmen einer Buchung an das TIM übergeben wird, muss die Zeichenersetzung durchgeführt werden.

Dazu sind die folgenden Schritte in der hier definierten Reihenfolge abzuarbeiten:

- Sofern die Ausdrucklänge auf dem Kassenbeleg 16 Zeichen unterschreitet:
  Kürzen der Zeichenkette auf Ausdrucklänge
- nicht druckbare Zeichen und Leerzeichen (ASCII Zeichen < 0x21 und = 0x7F) werden ausgelassen

- Ersetzung von: ABCDEFGHIJKLNOPQRSTUVWXYZ
  zu : abcdefghijklnopqrstuvwxyz
- erlaubte Zeichen: #0123456789abcdefghijklmnopqrstuvwxyz
- alle anderen Zeichen werden durch das Ersetzungszeichen ersetzt: #
- die Zeichenkette wird nach 16 Zeichen abgeschnitten

Vor dem Ablegen der Datensätze in die XML-Exportdatei muss Punkt 1 abgearbeitet sein (siehe Dokument → INSIKA Exportformat). Für möglichst verständliche Bezeichnungen in der Exportdatei sollten die weiteren Schritte erst bei der Verifikation durchgeführt werden.

Die Zeichenersetzung ist so gestaltet, dass nur der erste Durchlauf den Datensatz verändert. Jeder weitere Durchlauf führt zu keinen Veränderungen am Datensatz.

Weitere von der Zeichenersetzung betroffene Datensätze finden sich ggf. in der Beschreibung der Profile.

6.3 Rundung

Die Rundung wird kaufmännisch auf ganze Werte der kleinsten Währungseinheit (hier: 1 Euro-Cent) durchgeführt (siehe auch DIN 1333, Feb. 1992).

Zu einer positiven Zahl werden 0,5 der kleinsten Währungseinheit addiert und in dem Ergebnis werden die Ziffern hinter dem Komma weggelassen. Bei einer negativen Zahl wird ihr Betrag nach der zuvor beschriebenen Vorschrift gerundet. Vor den gerundeten Betrag wird das Minuszeichen gesetzt.

7 Informationen zur Signaturverifikation

Mit den in diesem Kapitel dargestellten Informationen lässt sich die Signaturverifikation durchführen. Für eine Basis-Integration zur Signaturerstellung mit dem TIM sind diese Informationen zunächst nicht nötig.

7.1 Hashvorschrift TRANSACTION

Zur Berechnung der Signaturen für Buchungen und frei wählbare Datensätze werden auf dem TIM die übergebenen Datenobjekte zunächst entsprechend der Reihenfolge in Tabelle 7-1 bzw. Tabelle 7-2 geordnet. Als erster Schritt des ECDSA-Verfahrens wird auf dem TIM über diese Daten ein SHA-1/SHA-256 Hashwert, siehe Fußnote 1, gebildet, der anschließend signiert wird.

7.1.1 TRANSACTION (Buchung)

Die Datenobjekte in Tabelle 7-1 sind signaturrelevant, d.h. sie gehen direkt in die Signatur ein. Alle Datenobjekte werden als TLV kodiert (→ 2.1).

Tabelle 7-1: Hashvorschrift TRANSACTION

Tag	Length (Byte)	Value	ggf. nicht übertragen[20]	Reihenfolge
CDh	4	Datum → 2.6.15		1
CEh	2	Uhrzeit → 2.6.16		2
C4h	1..32	Steuerpflichtigen-ID → 2.6.6		3
C5h	1..4	Lfd. Nummer des TIM → 2.6.7		4
C6h	1..16	Bedieneridentifikation → 2.6.8		5
C7h	20/32	Hashwert der Positionsdaten → 2.6.9		6
C9h	0	Merker: „Exklusiv Steuer“ → 2.6.13	X	7
CAh	0	Merker: „Trainings Modus“ → 2.6.12	X	8
D7h	0	Merker „Lieferschein“ → 2.6.13	X	0
CBh	1..4	Sequenznummer der Buchung → 2.6.14		9
E1h	6..12	Container 1 → 2.6.21	X	10 .. 39[21]
D8h	1..6	Umsatz → 2.6.18		
DBh	1..2	Umsatzsteuersatz → 2.6.19		
D6h	1..6	Umsatz Agenturgeschäft→ 2.6.18	X	

[20] Nullumsätze und nicht gesetzte Merker werden nicht übertragen.

[21] Reihenfolge entsprechend aufsteigender Container-Nummer 1-6, nicht gebuchte Container gehen nicht in den Hash ein

Tag	Length (Byte)	Value	ggf. nicht übertragen[20]	Reihenfolge
		…	X	
E6h	6..12	Container 6 → 2.6.21	X	
D8h	1..6	Umsatz → 2.6.18		
DBh	1..2	Umsatzsteuersatz → 2.6.19		
D6h	1..6	Umsatz Agenturgeschäft→ 2.6.18	X	

Der Hashwert wird über die Umsätze und Merker gebildet, die dem Befehl übergeben wurden. In zusammengesetzten Datenobjekten werden lediglich die Datenobjekte "Umsatz" (D8h), "Umsatzsteuersatz" (DBh), "Umsatz Agenturgeschäft" (D6h), jedoch nicht die Datenobjekte "Negativumsatz" (D9h) und "Umsatzsteuer" (DAh) verwendet.

Wurde in einem Umsatzcontainer das Feld "Umsatz" (D8h) nicht übergeben, wird es dennoch in die Hashwertbildung einbezogen. In diesem Fall wird der Wert 0 mit minimaler Länge kodiert (D8 01 0C) und gehasht. Andere nicht übergebene Umsätze oder Merker werden vom TIM nicht hinzugefügt.

7.1.2 TR Data, TR Tax Payer, TR Time Stamp

Die Datenobjekte in Tabelle 7-2 sind in Abhängigkeit von der Befehlsvariante signaturrelevant, d.h. sie gehen direkt in die Signatur ein. Alle Datenobjekte werden als TLV kodiert (→ 2.1).

Tabelle 7-2: Hashvorschrift TR Data, TR Tax Payer, TR Time Stamp

Tag	Length (Byte)	Value	ggf. nicht übertragen	Reihenfolge
CDh	4	Datum → 2.6.15	X	1
CEh	2	Uhrzeit → 2.6.16	X	2
C4h	1..32	Steuerpflichtigen-ID → 2.6.6	X	3
C5h	1..4	Lfd. Nummer des TIM → 2.6.7	X	4
C7h	20/32	Hashwert der zu signierenden Daten		5
CBh	1..4	Sequenznummer der Buchung → 2.6.14		6

7.2 Hashvorschrift REPORT

Zur Berechnung der Signaturen für Tagesabschlüsse werden die mit dem Befehl REPORT Signed, REPORT TIM Activate oder REPORT TIM Deactivate zurückgegebenen TLV-Objekte entsprechend der Tabelle 7-3 gehasht und anschließend signiert.

Die Felder "Umsatz" (D8h) und "Negativumsatz" (D9h) werden immer dann gehasht, wenn ein Umsatzcontainer bebucht wurde, selbst wenn die jeweilige Umsatzsumme den Wert 0 ausweist. Ein Nullumsatz wird mit minimaler Länge kodiert (Dx 01 0C) und gehasht.

Tabelle 7-3: Hashvorschrift REPORT

Tag	Length (Byte)	Value	ggf. nicht übertragen[22]	Reihenfolge
CDh	4	Datum → 2.6.15		1
CEh	2	Uhrzeit → 2.6.16		2
D4h	20/32	TIM Hashwert der Tagesabschluss-Positionen	X	3
C0h	1	TIM Lebenszyklus → 2.6.2		4
C4h	1..32	Steuerpflichtigen-ID → 2.6.6		5
C5h	1..4	Lfd. Nummer des TIM → 2.6.7		6
CCh	1..4	Sequenznummer des Tagesabschluss → 2.6.14		7
D2h	1..4	Sequenznummer der ersten Buchung → 2.6.14		8
D3h	1..4	Sequenznummer der letzten Buchung → 2.6.14		9
E1h	6..34	Container 1 → 2.6.21	X	10-57
D8h	1..11	Umsatz → 2.6.18		
D9h	1..11	Negativumsatz → 2.6.18		
DBh	1..2	Umsatzsteuersatz → 2.6.19		
DDh	0	Merker Umsatzüberlauf → 2.6.12	X	
DEh	0	Merker Änderung Umsatzsteuersatz → 2.6.12	X	
		…	X	
E6h	6..34	Container 6 → 2.6.21	X	
D8h	1..11	Umsatz → 2.6.18		
D9h	1..11	Negativumsatz → 2.6.18		
DBh	1..2	Umsatzsteuersatz → 2.6.19		
DDh	0	Merker Umsatzüberlauf → 2.6.12	X	
DEh	0	Merker Änderung Umsatzsteuersatz → 2.6.12	X	
E7h	6..23	Container Agenturgeschäft → 2.6.21	X	

[22] Nullumsätze und nicht gesetzte Merker werden nicht übertragen.

Tag	Length (Byte)	Value	ggf. nicht übertragen[22]	Reihenfolge
D8h	1..11	Umsatz → 2.6.18		
DCh	1..4	Zähler der Buchungen → 2.6.20		
DDh	0	Merker Umsatzüberlauf → 2.6.12	X	
E8h	6..23	Container Lieferschein → 2.6.21	X	
D8h	1..11	Umsatz → 2.6.18		
DCh	1..4	Zähler der Buchungen → 2.6.20		
DDh	0	Merker Umsatzüberlauf → 2.6.12	X	
E9h	6..21	Container Training → 2.6.21	X	
D8h	1..11	Umsatz → 2.6.18		
DCh	1..4	Zähler der Buchungen → 2.6.20		
DDh	0	Merker Umsatzüberlauf → 2.6.12	X	

Nicht gesetzte Merker und nicht gebuchte Umsatzsummenspeicher werden nicht in den Hash mit einbezogen.

In zusammengesetzten Datenobjekten (Tags E1h … E9h) werden lediglich die TLV-Objekte "Umsatz" (D8h), "Negativumsatz" (D9h), "Umsatzsteuersatz" (DBh), "Zähler der Buchungen" (DCh), "Merker Umsatzüberlauf" (DDh) und "Merker Änderung Umsatzssteuersatz" (DEh), das TLV-Objekt "Umsatzsteuer" (DAh) jedoch nicht verwendet. Nicht bebuchte Umsatzspeicher oder nicht gesetzte Merker werden vom TIM nicht hinzugefügt.

7.3 Hash- und Signaturverfahren

Das TIM verwendet ausschließlich offene und standardisierte Hash- und Signaturverfahren.

Die beim TIM V.2.1.0 verwendete Hashfunktion SHA-1/SHA-256 (Secure Hash Algorithm), siehe Fußnote 1, ist z.B.: in FIPS 180/FIPS 180-4 des NIST standardisiert. SHA-1 liefert kurze Hashwerte. Die theoretisch möglichen Kollisionsangriffe setzen voraus, dass große Datenmengen gehasht werden bei denen ein nennenswerter Teil der Daten unerkannt verändert werden könnte. Dies ist bei den durch INSIKA gesicherten Daten nicht der Fall. Dennoch wurde bei den TIM 2.1.0 SHA-256 als Standardhash für zukünftige Anwendungen und Erweiterungen festgelegt.

Das auf dem TIM V.2.1.0 verwendete Signaturverfahren ECDSA (Elliptic Curve Digital Signature Algorithm) ist in ANSI X9.62 bzw. FIPS 186 standardisiert.

Signierte Buchungen lassen sich mit dem Befehl VERIFY SIGNATURE (→ 3.6) auf dem TIM verifizieren. Unter Zuhilfenahme der Hashvorschriften (→ 7) lassen sich Anwendungen erstellen, die die Verifikation von signierte Buchungen und Tagesabschlüssen erlauben.

Beim Befehl TRANSACTION werden auf dem TIM folgende Schritte durchgeführt. Die übergebenen TLV-Objekte werden um die vom TIM bereitgestellten TLV-Objekte ergänzt. Anschließend werden die TLV-Objekte entsprechend der Hashvorschrift (→ 7.1) geordnet und gewandelt. Über diese Objekte wird ein Hashwert gebildet und anschließend mit Hilfe des privaten Schlüssels signiert.

Beim Befehl REPORT werden auf dem TIM die folgenden Schritte durchgeführt. Die TLV-Objekte der Anfrage und die intern ermittelten TLV-Objekte werden entsprechend der Hashvorschrift (→ 7.2) geordnet. Über diese Objekte wird ein Hashwert gebildet und anschließend mit Hilfe des privaten Schlüssels signiert.

7.4 Domainparameter

Das TIM V.2.1.0 nutzt die folgenden ECDSA Domainparameter für ECDSA-192:

```
P:  0xFFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFFFFF FFFFFFFF
a:  0xFFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFFFFF FFFFFFFC
b:  0x64210519 E59C80E7 0FA7E9AB 72243049 FEB8DEEC C146B9B1
Gx: 0x188DA80E B03090F6 7CBF20EB 43A18800 F4FF0AFD 82FF1012
Gy: 0x07192B95 FFC8DA78 631011ED 6B24CDD5 73F977A1 1E794811
n:  0xFFFFFFFF FFFFFFFF FFFFFFFF 99DEF836 146BC9B1 B4D22831
h:  0x1
```

Diese Domainparameter sind in verschiedenen Standards definiert und werden dort unter den Namen "ANSIp192r1", "prime192v1", "P-192" bzw. "secp192r1" geführt (siehe ANSI X9.62, FIPS 186 etc.).

Für ECDSA-256 werden dagegen die Domänparameter

NIST P-256 (nach NIST 186-4) verwendet:

```
p =  0xFFFFFFFF 00000001 00000000 00000000 00000000 FFFFFFFF FFFFFFFF FFFFFFFF
a =  0xFFFFFFFF 00000001 00000000 00000000 00000000 FFFFFFFF FFFFFFFF FFFFFFFC
b =  0x5AC635D8 AA3A93E7 B3EBBD55 769886BC 651D06B0 CC53B0F6 3BCE3C3E 27D2604B
Gx = 0x6B17D1F2 E12C4247 F8BCE6E5 63A440F2 77037D81 2DEB33A0 F4A13945 D898C296
Gy = 0x4FE342E2 FE1A7F9B 8EE7EB4A 7C0F9E16 2BCE3357 6B315ECE CBB64068 37BF51F5
n =  0xFFFFFFFF 00000000 FFFFFFFF FFFFFFFF BCE6FAAD A7179E84 F3B9CAC2 FC632551
h =  0x01
```

7.5 Format der Signatur

Die Signatur wird in einer Folge von zwei 192/256 Bit Binärzahlen r und s, siehe Fußnote 1 direkt aufeinander folgend zurückgegeben. Somit werden in dem TLV-Objekt "TIM Signatur" 48/64 Byte übertragen (→ 2.6.1).

7.6 Zertifikat und öffentlicher Schlüssel

Das Zertifikat auf dem TIM folgt den Festlegungen in ITU-T X.509v3. Es ist in einer ASN.1 Struktur definiert und ist auf dem TIM in binärer DER-Kodierung gespeichert.

Das Zertifikat hat die folgende ASN.1 Struktur:

```
Certificate ::= SEQUENCE  {
    tbsCertificate       TBSCertificate,
    signatureAlgorithm   AlgorithmIdentifier,
    signatureValue       BIT STRING  }
```

7.6.1 Länge des Zertifikats

Das folgende Beispiel zeigt, wie die Längeninformation aus dem Zertifikat gelesen werden kann. Der Anfang des Beispiel-Zertifikats lautet:

30h 82h 03h 38h 30h 82h 02h 20h A0h …

Das erste Byte "30h" kennzeichnet eine Sequenz der BER/DER Klasse "constructed universal". Die "82h" ist das initiale Byte des Längenfeldes, das die nachfolgenden zwei Bytes

anzeigt. Die Bytes "03h 38h" geben die Länge des folgenden Datenteils an. Damit folgen also 824 Byte. Das gesamte Zertifikat ist damit 828 Byte lang.

7.6.2 Öffentlicher Schlüssel im Zertifikat

Das im Zertifikat enthaltene Objekt **TBSCertificate** hat folgende ASN.1 Struktur:

```
TBSCertificate          ::=  SEQUENCE {
    Version                  [0] EXPLICIT Version DEFAULT v1,
    serialNumber             CertificateSerialNumber,
    signature                AlgorithmIdentifier,
    issuer                   Name,
    validity                 Validity,
    subject                  Name,
    subjectPublicKeyInfo     SubjectPublicKeyInfo,
    issuerUniqueID           [1] IMPLICIT UniqueIdentifier OPTIONAL,
    subjectUniqueID          [2] IMPLICIT UniqueIdentifier OPTIONAL,
    extensions               [3] EXPLICIT Extensions OPTIONAL
}
```

Das Zertifikat enthält den öffentlichen Schlüssel (Public Key). Die Schlüssellänge beträgt 192/256 Bit, siehe Fußnote 1. Da der öffentliche Schlüssel einen Punkt auf einer elliptischen Kurve darstellt, wird er in einer Folge von zwei direkt aufeinander folgenden 192/256 Bit Binärzahlen, siehe Fußnote 1 kodiert. Der Umfang beträgt damit 48/64 Byte, s. Fußnote 1.

Im Zertifikat ist der Public Key im Objekt **SubjectPublicKeyInfo** abgelegt, das die folgende ASN.1 Struktur besitzt:

```
SubjectPublicKeyInfo    ::=  SEQUENCE {
    algorithm                AlgorithmIdentifier,
    subjectPublicKey         BIT STRING
}
```

Das enthaltene Objekt **AlgorithmIdentifier** hat folgende ASN.1 Struktur:

```
AlgorithmIdentifier     ::=  SEQUENCE {
    algorithm                OBJECT IDENTIFIER,
    parameters               ANY DEFINED BY algorithm OPTIONAL
}
```

Der OBJECT IDENTIFIER (OID) für ECDSA muss grundsätzlich dem id-ecPublicKey algorithm identifier entsprechend der Definition

id-public-key-type OBJECT IDENTIFIER ::= { ansi-X9.62 2 }

id-ecPublicKey OBJECT IDENTIFIER ::= { id-publicKeyType 1 }

und den namedCurve OBJECT IDENTIFIER enthalten.

Für das verwendete Signaturverfahren SHA1ECDSA mit den Domainparametern prime192v1 ist das { 1.2.840.10045.3.1.1 }. In der DER kodierten Form ergibt sich daraus die OID: "06h 08h 2Ah 86h 48h CEh 3Dh 03h 01h 01h" (siehe ITU-T X.690). Dem vorangestellt

Beispielhaft ist beim TIM V.2.1.0 für SHA1/ECDSA das Objekt SubjectPublicKeyInfo folgendermaßen kodiert:

```
…30h 49h
        30h 13h
                06h 07h 2Ah 86h 48h CEh 3Dh 02h 01h
                06h 08h 2Ah 86h 48h CEh 3Dh 03h 01h 01h
        03h 32h 00h 04h ..(48 Byte Public Key)..
…
```

Das erste Byte "30h" kennzeichnet eine Sequenz der BER/DER Klasse CONSTRUCTED UNIVERSAL. Das nachfolgende Byte "49h" zeigt die Länge an. Es folgen somit 73 Byte.

Die "30h" kennzeichnet wiederum eine Sequenz der BER/DER Klasse CONSTRUCTED UNIVERSAL mit der Länge "13h". Die "06h" zeigt einen OBJECT IDENTIFIER an. Das nächste Byte "08h" gibt die Länge an. Darauf folgt nun der OID. Das nächste Objekt kennzeichnet optionale Parameter.

Die "03h" zeigt einen BIT STRING der BER/DER Klasse UNIVERSAL an. Das nachfolgende Byte "32h" zeigt die Länge an. Es folgen somit 50 Byte. Dem Public Key werden die Bytes "00h 04h" vorangestellt. Das Byte "00h" signalisiert, wie viele unbenutzte Bits im letzten Oktett des BIT STRING enthalten sind. Das Byte "04h" signalisiert, dass es sich um einen unkomprimierten Schlüssel handelt. Die darauf folgenden 48 Byte ist der Public Key.

Für SHA256/ECDSA ist der namedCurve OBJECT IDENTIFIER mit den Domänparametern NIST P-256 {1.2.840.10045.3.1.7}. In der DER kodierten Form ergeben sich daraus die OID: "06h 08h 2Ah 86h 48h CEh 3Dh 03h 01h 07h" und siehe ITU-T X.690).

Beispielhaft ist beim TIM V.2.1.0 für SHA256/ECDSA das Objekt `SubjectPublicKeyInfo` folgendermaßen kodiert:

```
30h 59h
          30h 13h
                06h 07h 2Ah 86h 48h CEh 3Dh 02h 01h
                06h 08h 2Ah 86h 48h CEh 3Dh 03h 01h 07h
          03h 42h 00h 04h <64 Byte Public Key>
```

Hinweis:
Der OID zeigt nur das Signaturverfahren und die verwendeten Domainparameter an. Um das Objekt `SubjectPublicKeyInfo` zu lesen, muss ein vollständiges Parsen des X.509-Zertifikats anhand der ASN.1-Struktur und der ASN.1-Objekte (anhand von Tag und Länge) vorgenommen werden! (siehe dazu ITU-T X.509v3)

8 Daten auf dem TIM

8.1 Personalisierungsdaten des TIM

Durch die ausgebende Stelle wird das TIM auf den Steuerpflichtigen personalisiert. Dazu werden die Daten gemäß Tabelle 8-1 auf dem TIM eingetragen:

Tabelle 8-1: Personalisierungsdaten des TIM

Personalisierungs-daten	Name	Tag	Befehl zum Auslesen
Lebenszyklus des TIM	TIM_LIFECYCLE	C0h	GET DATA TIM Status / GET DATA TIM Status extended
Transport-PIN	TIM_TRANSPORT_PIN	C3h	-
Steuerpflichtigen-ID	TIM_TP_ID	C4h	GET DATA TIM Status extended / TRANSACTION / REPORT
Lfd. Nummer des TIM bezogen auf eine TIM_TP_ID	TIM_TP_ID_NO	C5h	GET DATA TIM Status extended / TRANSACTION / REPORT
Währungscode	TIM_CURRENCY	C8h	GET DATA TIM Status extended
Personalisierungs-datum	(unsigned BCD)	-	-
Erster Monat, in den gebucht werden kann	TIM_DATE	CDh	GET DATA TIM Booked Months
Letzter buchbarer Monat [23]	TIM_DATE	CDh	GET DATA TIM Status extended
Länderkennzeichen	TIM_COUNTRY_CODE	D5h	GET DATA TIM Status extended
Anzahl der buchbaren Monate	(binär)	-	-
Zertifikat	(Datei EF_CERT auf TIM)	-	READ CERTIFICATE

8.2 Umsatzspeichermodell des TIM

Auf dem TIM werden sog. Umsatzspeicher gehalten. In diesem Abschnitt wird die Struktur und der Inhalt dieser Summenspeicher erläutert, die in Abbildung 8-1 schematisch dargestellt sind. Die Beschreibung dieser Strukturen soll das Verständnis der vom REPORT Befehl gelieferten Daten erleichtern.

Jeder erfolgreich durchgeführte Befehl TRANSACTION aktualisiert die Umsatzspeicher auf dem TIM. Durch den Befehl REPORT werden diese Umsatzspeicher ausgelesen.

[23] Die Laufzeit der Karte wird bei der Personalisierung festgelegt

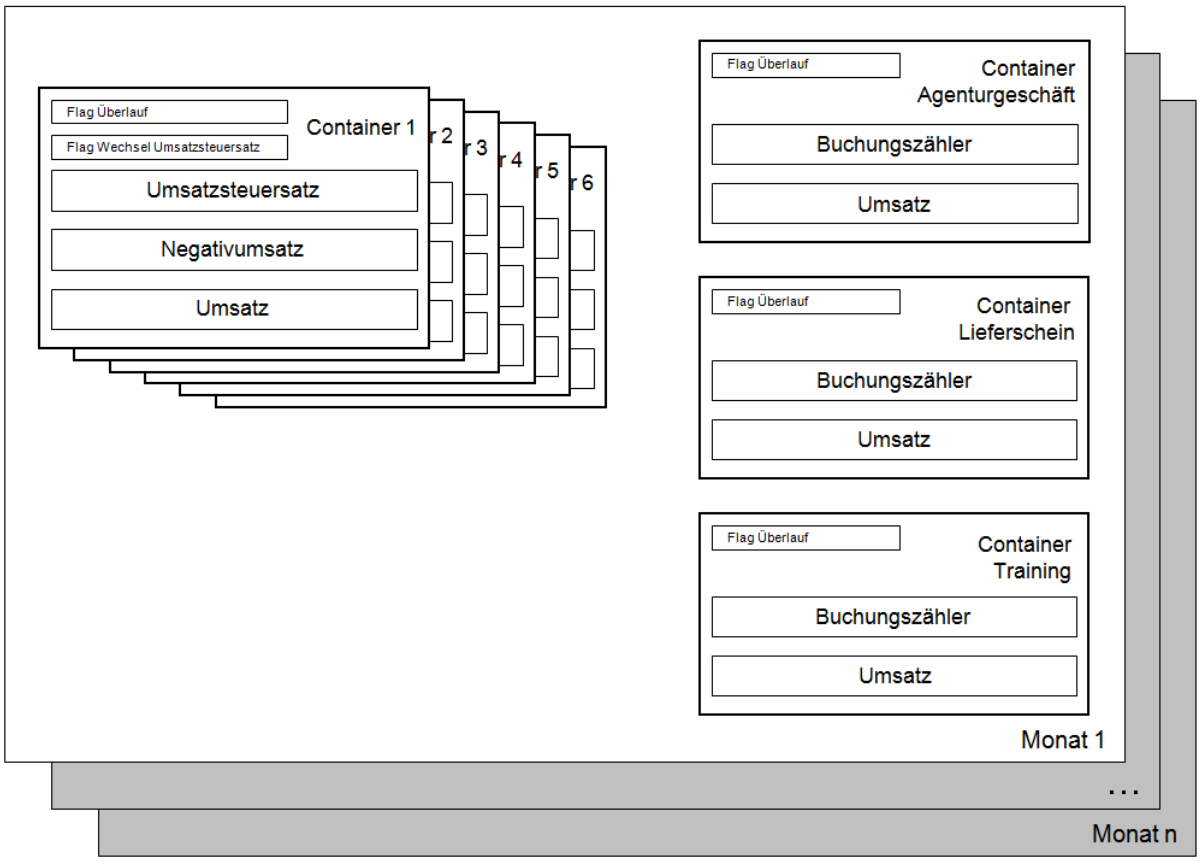

Abbildung 8-1: Umsatzspeichermodell des TIM

Jeder Monat wird auf dem TIM separat gespeichert. Mit dem Befehl REPORT Span lassen sich die Monate einzeln ausgeben. Die Anzahl der Monate wird von der ausgebenden Stelle während der Personalisierung eingetragen.

Die Befehle REPORT Signed und REPORT Unsigned geben die Summen über alle bebuchten Monate zurück.

Für jeden Monat besitzt das TIM neun verschiedene Container. Die Container 1-6 bilden die Umsatzsteuerklassen (→ 6.1) direkt ab. Zusätzlich werden die Container Agenturgeschäft, Lieferschein und Training auf dem TIM gehalten. Nachfolgend werden die Container einzeln erläutert.

8.2.1 Container 1..6

In den Containern 1..6 werden die umsatzsteuerbezogenen Entgelte der Buchungen summiert. Die Container 1..6 bilden die Umsatzsteuerklassen (→ 6.1) direkt ab.

Die monetären Werte (Umsatz und Negativumsatz) werden brutto – also inklusive Umsatzsteuer – gespeichert.

Bei Nettobuchungen werden die Umsätze vor der Addition vom TIM entsprechend umgerechnet. Um hierbei den Einfluss von Rundungsfehlern zu verringern, wird bei dieser Berechnung auf eine erweiterte Genauigkeit von 0,0001 der kleinsten Währungseinheit kaufmännisch gerundet (→ 6.3). In den Containern 1..6 werden der Umsatz und der Negativumsatz in dieser erweiterten Genauigkeit gespeichert. Die erweiterte Genauigkeit dient ausschließlich der internen Summenhaltung und wird nicht ausgegeben. Beim Auslesen der Summen durch einen REPORT Befehl wird auf die kleinste Währungseinheit kaufmännisch gerundet.

Das Feld Umsatz entspricht dem nach Steuersätzen und einzelnen Steuerbefreiungen aufgeschlüsselten Entgelt für die Lieferung oder sonstige Leistung. Da es sich hierbei um die Gesamtsumme der Buchung handelt, sind sowohl Agenturumsätze als negative Umsätze berücksichtigt. Buchungen im Lieferschein- oder Trainingsmode aktualisieren lediglich die Lieferschein- bzw. Trainingsumsatzspeicher.

Bei der ersten Buchung eines neuen Monats wird der Umsatzsteuersatz in den entsprechenden Container eingetragen. Falls im laufenden Monat ein neuer Wert für den Umsatzsteuersatz gespeichert wird, wird der entsprechende Merker "Änderung Umsatzsteuersatz" gesetzt. Veränderungen des Umsatzsteuersatzes werden üblicherweise nur zu Monatswechseln durchgeführt. Für eine Prüfung ist jederzeit bekannt, welcher Umsatzsteuersatz in welchem Monat gültig ist. Das TIM überprüft den übergebenen Umsatzsteuersatz nicht in der Höhe sondern lediglich die darauf basierende Berechnung der Umsatzsteuer. (siehe auch Umsatzsteuerklassen → 6.1)

Negativumsätze in Buchungen werden im Umsatz übergeben (100 Euro gebucht, 10 Euro Warenrücknahme = 90 Euro Umsatz). Die Negativumsätze werden umsatzsteuerbezogen in dem jeweiligen Container an das TIM übergeben. Negativumsätze werden positiv übertragen.

Bei einer Buchung führt das TIM eine Plausibilitätsprüfung hinsichtlich Umsatz der Buchung (Summe USt-bezogenes Entgelt der Buchung) in Bezug auf den Negativumsatz der Buchung (Summe USt bezogene Entgelte der negativen Buchungspositionen) durch. Bei einem negativen Umsatz muss der Negativumsatz größer oder gleich dem absoluten Betrag des Umsatzes sein. Dadurch wird sichergestellt, dass Umsatzverkürzungen durch negative Gesamtsummen auch bei Verlust des Journals erkannt werden.

8.2.2 Container Agenturgeschäft E7h

Bei Agenturumsätzen handelt es sich um Lieferungen oder Leistungen im Namen und auf Rechnung eines Dritten. Für jeden Monat wird ein separater Container angelegt.

Agenturumsätze fließen in die Umsätze der Container der zugehörigen Umsatzsteuerklassen ein und werden folglich über diese mitsigniert. Dem TIM werden Agenturumsätze im Befehl TRANSACTION zum Aktualisieren der Agentursummen im Container E7h im Container der entsprechenden Umsatzsteuerklasse übergeben, und dadurch in die Signatur der Buchung einbezogen (vgl.→ 7.1). Wird die Agentursumme durch die Kasse nicht ordnungsgemäß an das TIM übergeben, kann dem Steuerpflichtigen kein Vorteil entstehen, da die Umsätze dann als regulärer Umsatz aufgefasst werden.

Agenturumsätze unterliegen in der Regel einem „Vier-Augen“-Prinzip. Hierbei haben zwei Parteien ein Interesse an der Integrität der Daten. Die Kontrolle wird in der Regel über nachgeschaltete Systeme durchgeführt. Aus Gründen der Plausibilisierung wird die Anzahl der Buchungen, in denen Agenturumsätze aufgetreten sind, im "Zähler der Buchungen Agenturgeschäft" erfasst.

8.2.3 Container Lieferschein E8h

Lieferscheine sind Geschäftsvorfälle, bei die Lieferung oder Leistung dokumentiert werden soll, die Rechnungserstellung aber zu einem späteren Zeitpunkt erfolgt. Es handelt sich dabei also nicht um steuerpflichtige Umsätze so dass sie auch nicht in die Umsätze der Container der zugehörigen Umsatzsteuerklassen auf dem TIM einfließen. Folglich werden sie auch nicht bei einem REPORT über diese mitsigniert.

Lieferscheine müssen immer als separate Geschäftsvorfälle erfasst werden. Die Kombination mit steuerpflichtigen Umsätzen in einer Buchung ist nicht möglich. Die Erfassung kann wahlweise mit oder ohne Preisinformationen erfolgen, in letzterem Fall wird im Umsatzcontainer Lieferschein lediglich die Anzahl der signierten Lieferscheine erfasst. Da die Rechnungsstellung in einem nachgeschalteten System erfolgt, in dem das Entgelt noch durch unterschiedliche Parameter beeinflusst werden kann (Rabatte u.ä.), hat diese Summe eher informativen Charakter.

Dem TIM werden Lieferscheindaten im Befehl TRANSACTION mit gesetztem Merker Lieferschein übergeben. Sofern Preisinformationen übergeben werden sollen, erfolgt das über die Container der entsprechenden Umsatzsteuerklasse. TIM-intern werden die in der Buchungsanfrage in den Containern E1h bis E6h übergebenen Umsätze als Bruttoumsatz im Container Lieferschein (E8h) summiert. Sie werden nicht in die Summenspeicher der Umsatzcontainer „Umsatz 1 bis 6“ übernommen. Bei gleichzeitig gesetzten Merkern Lieferschein und Training erfolgt eine Verbuchung als Training.

8.2.4 Container Training E9h

Bei als Training gekennzeichneten Buchungsanfragen, s. 3.4.1, werden die in E1h bis E6h übergebenen Umsätze nicht in Container 1..6 übernommen, sondern als eine Summe in den Summenspeicher Trainingsumsatz aufaddiert. Da es sich hierbei um Buchungen handelt, die keinen Geschäftsvorfall abbilden und damit keine Lieferung oder sonstige Leistung erfolgt, werden die Umsätze nicht USt-bezogen abgebildet. Da jedoch speziell in diesen Buchungen ein nennenswertes Risiko bzw. Manipulationspotenzial steckt, werden die Umsätze in der Signatur der Buchung erfasst. Aus Gründen der Plausibilisierung wird zusätzlich die Anzahl der Trainingsbuchungen im "Zähler der Buchungen Training" erfasst.

Für jeden Monat wird ein separater Container angelegt.

9 Profile

Durch Profile lassen sich verschiedene praktische Anwendungsfälle auf das INSIKA-Verfahren abbilden. Deren Unterschiede liegen vor allem in:

- dem Inhalt und Aufbau der Buchungspositionen,
- eventuellen Zusatzdaten für Tagesabschlüsse und
- dem Mechanismus zur Kontrolle der korrekten Anwendung des Systems.

Auch die Prüfung der Daten muss profilspezifisch erfolgen – dieser Aspekt wird in diesem Dokument jedoch nicht behandelt.

Die Schnittstelle zum TIM ist unabhängig vom Profil. In jeder Anwendung wird genau ein Profil verwendet. Der Wechsel des Profils im laufenden Betrieb ist nicht sinnvoll und daher nicht vorgesehen.

9.1 Buchungspositionen

Das Profil definiert die Datenobjekte der Buchungspositionen (BP), über die dann ein Hashwert gebildet wird. Im Rahmen einer Buchung wird dieser Hashwert (→ 2.6.9) an das TIM übergeben und signiert (→ 3.4). Damit gehen diese Datenobjekte indirekt in die Signatur mit ein. Somit kann eine große Zahl von Datenobjekten signiert werden, ohne dass diese auf der TIM Schnittstelle übertragen werden müssen.

Die Hauptaufgabe der Buchungspositionen ist es, die verschiedenen Umsatzwerte, die bei der Buchung an der TIM übergeben werden, nachvollziehbar darzustellen.

Eine Abbildung der Buchungspositionen in TLV-Objekten ist der sinnvollste Weg, da diese Darstellung standardisiert ist und die nötigen Mechanismen bereits für die Kommunikation mit dem TIM vorhanden sind. Alternative Abbildungsverfahren sind jedoch nicht ausgeschlossen.

9.2 Daten Tagesabschluss

Im einfachsten Fall werden die Inhalte eines Tagesabschlusses (→ 3.5) vollständig vom TIM geliefert (basierend auf den Umsatzspeichern des TIM). Es kann jedoch sinnvoll sein, zusätzliche Informationen aufzuzeichnen und diese zu ihrer Absicherung in die Signatur einzubeziehen.

Dazu kann der gleiche Mechanismus wie bei den Buchungspositionen verwendet werden. Auch hier wird mit Hilfe der im Profil definierten Abbildungsvorschrift ein Hashwert über die Zusatzinformationen gebildet (→2.6.10) und dem TIM übergeben.

9.3 Kontrollmechanismus

Für jeden Anwendungsfall von INSIKA und damit für jedes Profil ist zu definieren, wie eine Überwachung der korrekten Nutzung des Systems erfolgen soll. Das sinnvollste Mittel dazu ist i.d.R. die Ausgabe von signierten, überprüfbaren Belegen – diese können in Papierform ausgegeben oder auch elektronisch erstellt und auf einem Server abgelegt werden.

Wenn möglich, sollte die Kontrolle dabei ausschließlich anhand des Beleges und eines Zugriffs auf die kryptografischen Zertifikate möglich sein. Dazu muss der Beleg folgende Anforderungen erfüllen:

- Aus dem Beleg müssen sich die Buchungspositionen so rekonstruieren lassen, dass sie in Inhalt, Form und Reihenfolge exakt den Daten zum Zeitpunkt der Signatur entsprechen. In der Folge ergibt sich dann in beiden Fällen der gleiche Hashwert.
- Alle Daten, die nicht in den Hashwert der Buchungspositionen einfließen, aber an das TIM übergeben (z.B. Datum und Uhrzeit) bzw. von diesem zurückgeliefert werden (z.B. die Steuerpflichtigen-ID und die Signatur) müssen ebenfalls exakt aus dem Beleg reproduzierbar sein.
- Für eine vereinfachte Verifikation (sinnvoll bei gedruckten Belegen) kann im Einzelfall auf eine Überprüfung des Hashwertes der Buchungspositionen verzichtet werden. Man verzichtet dabei also auf die Prüfung der einzelnen Buchungspositionen und verifiziert lediglich Gesamtsummen des Belegs, Datum, Uhrzeit usw. Da für diese Variante der Verifikation der Hashwert erforderlich ist, muss er aus dem Beleg hervorgehen.
- Eine (weitgehend) automatische Verifikation eines Belegs ist die ideale Lösung. Bei elektronischen Dokumenten ist dies ohne weiteres möglich – bei gedruckten Belegen bietet sich die Codierung der erforderlichen Daten in einem maschinenlesbaren Code (z.B. QR-Code) an. Aus Kapazitätsgründen wird man hier auf die Codierung der Buchungspositionen selbst verzichten und stattdessen deren Hashwert aufnehmen.

Da sich aufgrund technischen Einschränkungen bei bestimmten Druckern Probleme mit diesen Anforderungen ergeben können (wenn z.B. ein Drucker nur Großbuchstaben druckt oder bestimmte Akzente nicht darstellen kann), sollte bei Texten vor der Hashwertberechnung unbedingt eine Zeichensetzung (→ 6.2) durchgeführt werden.

10 Anhang

10.1 Beispiele

Hinweis:
Die folgenden Beispiele beziehen sich alle auf das Profil Registrierkasse.

10.1.1 Beispiel: Buchung 1

Die Buchungspositionen des Profils Registrierkasse werden entsprechend Profilfestlegungen kodiert. Nach der Hashvorschrift für Buchungspositionen wird dann ein SHA-1 Hashwert berechnet: (Die Buchungspositionen werden nicht auf der TIM-Schnittstelle übertragen.) Bei Verwendung der neuen Kryptoalgorithmen erhöht sich lediglich die Anzahl der Zeichen des Hashwerts von 20 auf 32.

Buchungspositionen gemäß Profil Registrierkasse (hex)*	**Inhalt**	
A0h 04h 30h 2Eh 30h 38h	ITEM Menge/Anz.:	"0.08"
A1h 02h 6Bh 67h	ITEM Einheit:	"kg"
A2h 0Bh 6Ah 61h 70h 61h 6Eh 73h 65h 6Eh 63h 68h 61h	ITEM Name:	"japansencha"
B2h 02h 47h 2Ch	ITEM Preis 2:	"+472"
A0h 01h 31h	ITEM Menge/Anz.:	"1"
A2h 10h 74h 65h 65h 6Bh 61h 6Eh 6Eh 65h 67h 75h 73h 73h 65h 69h 73h 65h	ITEM Name:	"teekannegusseise"
B1h 03h 04h 99h 0C	ITEM Preis 1:	"+4990"
A0h 01h 31h	ITEM Menge/Anz.:	"1"
A2h 09h 31h 30h 23h 72h 61h 62h 61h 74h 74h	ITEM Name:	"10#rabatt"
AAh 00h	ITEM Merker Rabatt/Aufschlag	
B1h 02h 49h 9Dh	ITEM Preis 1:	"-499"
5Eh F0h 13h F1h A1h F3h 3Bh 00h FBh 18h 00h 9Bh BCh 51h 63h 8Bh 36h 4Ch 6Eh 28h	SHA-1 Hashwert der Buchungspositionen	

* Absätze und Einzüge dienen nur der anschaulichen Darstellung

Nach Berechnung des Hashwert der Buchungspositionen wird der Befehl TRANSACTION zusammengestellt und an das TIM übertragen. Das TIM signiert die Daten und liefert die Signatur zurück. Bei Verwendung der neuen Kryptoalgorithmen erhöht sich lediglich die Anzahl der Zeichen der Signatur von 48 auf 64.

Befehl/Antwort (hex) *	Inhalt
80h 40h 00h 00h 50h	Befehl TRANSACTION LC = 80 Byte
CDh 04h 20h 10h 02h 28h CEh 02h 23h 59h C6h 09h 6Fh 70h 65h 72h 61h 74h 6Fh 72h 35h	Datum: "2010-02-28" Zeit: "23-59" Bediener "operator5"
C7h 14h 5Eh F0h 13h F1h A1h F3h 3Bh 00h FBh 18h 00h 9Bh BCh 51h 63h 8Bh 36h 4Ch 6Eh 28h	Hashwert der Buchungspositionen
C8h 02h 03h D2h	Währungscode: 978 (Euro)
E1h 11h D8h 03h 04h 49h 1Ch D9h 02h 49h 9Ch DAh 02h 71h 7Ch DBh 02h 19h 00h	Container 1 Umsatz: "+4491" NegUmsatz: "+499" Umsatzsteuer: "+717" Umsatzsteuersatz: "1900"
E2h 0Ch D8h 02h 47h 2Ch DAh 02h 03h 1Ch DBh 02h 07h 00h	Container 2 Umsatz: "+472" Umsatzsteuer: "+31" Umsatzsteuersatz: "0700"
00h	LE = 00h
	A n t w o r t
C4h 0Fh 49h 4Eh 53h 49h 4Bh 41h 5Fh 54h 45h 53h 54h 5Fh 50h 54h 42h	TPID:"INSIKA_TEST_PTB"
C5h 01h 01h	TPIDNO: "1"
CBh 02h 27h C0h	Seq.No der Buchung: "10176"
9Eh 30h 47h 40h 88h BAh D5h 4Dh B9h 48h 5Ch 93h 19h 29h F3h 0Bh 54h C7h 28h 9Eh C2h 6Ch F0h F1h 2Ah C2h 75h 70h 42h A4h 42h E0h 8Dh B1h A4h 0Ah 88h 27h 2Eh C8h 4Ch E4h 8Dh 33h B1h 32h 35h 75h 12h 19h	Signatur
90h 00h	SW1/SW2, No Error

* Absätze und Einzüge dienen nur der anschaulichen Darstellung

10.1.2 Beispiel: Buchung 2

Profil-Daten:

Buchungspositionen gemäß Profil Registrierkasse (hex)*	Inhalt
A0h 05h 35h 34h 2Eh 30h 33h A1h 01h 6Ch A2h 06h 64h 69h 65h 73h 65h 6Ch ACh 00h B1h 03h 06h 21h 3C	ITEM QUANTITY: "54.03" ITEM UNIT: "l" ITEM NAME: "diesel" ITEM THIRDPARTY: ““ ITEM Preis 1: "+6213"
E0h 72h F8h C3h 1Dh 5Ch BDh 44h A8h C3h 7Bh 4Eh 80h DCh 63h 08h 16h 46h E2h 4Eh	SHA-1 Hashwert der Buchungspositionen bei SHA-256 32 Zeichen

* Absätze und Einzüge dienen nugr der anschaulichen Darstellung

Befehl TRANSACTION:

Befehl/Antwort (hex) *	Inhalt
80h 40h 00h 00h 3Dh	**Befehl TRANSACTION** LC = 61 Byte
CDh 04h 20h 17h 02h 01h	Datum: "2017-02-01"
CEh 02h 12h 00h	Zeit: "12:00"
C6h 03h 30h 30h 31h	Bediener: "001"
C7h 14h E0h 72h F8h C3h 1Dh 5Ch BDh 44h A8h C3h 7Bh 4Eh 80h DCh 63h 08h 16h 46h E2h 4Eh	Hashwert der Buchungspositionen bei SHA-256 hier 32 Zeichen
C8h 02h 03h D2h	Währungscode: 978 (Euro)
E1h 12h	Container 1
D8h 03h 06h 21h 3Ch	Umsatz: "+6213"
DAh 02h 99h 2Ch	Umsatzsteuer: "+992"
DBh 02h 19h 00h	Umsatzsteuersatz: "1900"
D6h 03h 06h 21h 3Ch	Umsatz Agenturgeschäft "+6213"
00h	LE = 00h
	A n t w o r t
C4h 10h 49h 4Eh 53h 49h 4Bh 41h 5Fh 54h 45h 53h 54h 5Fh 41h 44h 4Dh 5Ah	TPID:"INSIKA_TEST_ADMZ"
C5h 02h 03h E7h	TPIDNO: "999"
CBh 01h 02h	Seq.No der Buchung: "2"
9Eh 30h 5Fh 10h D9h 4Fh 9Bh D0h A4h 97h 0Bh EEh ACh 25h 96h 40h 50h CBh 29h BBh 3Eh 7Eh D2h A0h A1h AAh 02h F8h FDh B3h 5Eh FBh 82h 57h F5h E4h 5Fh 5Dh 9Fh 1Ah ACh 7Fh 94h FCh 58h 47h 6Dh 88h EBh 6Bh	Signatur 48 bzw. 64 Byte, siehe Fußnote 1
90h 00h	SW1/SW2, No Error

Anmerkung: Mögliche Verifikation des o.g. Datensatzes mit dem öffentlichen Schlüssel:

A87AD0A2D0B60C24F75DAE1CEFDABA64EBFEDDC603618683

B3C2B0944D317D14DCA2458DAA915577F1AEB62D8A886AD4

10.1.3 Beispiel: Tagesabschluss

Befehl/Antwort (hex) *	Inhalt
80h 42h 01h 00h 0Ah	**Befehl REPORT signed** LC = 10 Byte
CDh 04h 20h 09h 05h 01h CEh 02h 17h 37h	Datum "2009-05-01" Zeit "17-37"
00h	LE = 00h
	Antwort
C0h 01h 03h	Lebenszyklus "TIM_ACTIVATED"
C4h 0Dh 54h 50h 49h 44h 5Fh 54h 45h 53h 54h 5Fh 50h 54h 42h	TPID:"TPID_TEST_PTB"
CCh 01h 1Ah	TPIDNO: "26"
C5h 01h 03h	Seq.No Tagesabschluss: "3"
D2h 01h 01h	Seq.No erste Buchung: "1"
D3h 01h 15h	Seq.No letzte Buchung: "176"
E1h 0Eh	Container 1
D8h 03h 02h 49h 9Ch	Umsatz: "+2499"
D9h 03h 02h 52h 0Ch	Negativumsatz: "+2520"
DBh 02h 19h 00h	Umsatzsteuersatz: "1900"
9Eh 30h 4Bh A5h AEh E1h D4h E0h 10h ABh 37h 16h B4h 4Dh 78h 06h 2Bh 82h 14h 72h 3Fh 2Bh 4Bh 68h 06h 7Eh DCh F7h E5h 61h 69h 15h CAh 76h FBh 1Ch B5h 99h 71h 2Ah C9h C6h D7h F2h 97h 52h 46h 74h E9h 21h	Signatur 48 bzw. 64 Byte, siehe Fußnote 1
90h 00h	SW1/SW2, No Error

* Absätze und Einzüge dienen nur der anschaulichen Darstellung

10.1.4 Beispiel: READ CERTIFICATE

In diesem Beispiel wird das Zertifikat aus dem TIM gelesen. Dazu werden Blöcke von 128 Byte (LE=80h) angefordert. Der Offset (P1 und P2) des Befehls READ CERTIFICATE wird jeweils um 80h inkrementiert.

Sofern die Länge des Zertifikats nicht während dieser Befehlsfolge ausgewertet wird, kann auch bis zur Fehlermeldung 6A 86h gelesen werden. Um das X.509 Zertifikat zu erhalten, muss im Anschluss die Länge des Zertifikats ausgewertet werden.

Befehl/Antwort (hex) *	Inhalt
00h A4h 00h 0Ch 02h 11h 10h	**Befehl: SELECT FILE** LC = 2 Byte Data = 11 10h (EF_CERT) LE = --
90h 00h	**Antwort** SW1/SW2: No Error
00h B0h 00h 00h 00h 80h	**Befehl** **READ CERTIFICATE** Offset = 00 00h LC = 0 Byte LE = 80h
30h 82h 03h 60h 30h 82h 02h 48h A0h 03h 02h 01h 02h 02h 04h 00h 00h 04h 50h 30h 0Dh 06h 09h 2Ah 86h 48h 86h F7h 0Dh 01h 01h 05h 05h 00h 30h 81h 84h 31h 0Bh 30h 09h 06h 03h 55h 04h 06h 13h 02h 44h 45h 31h 2Eh 30h 2Ch 06h 03h 55h 04h 0Ah 0Ch 25h 50h 68h 79h 73h 69h 6Bh 61h 6Ch 69h 73h 63h 68h 2Dh 54h 65h 63h 68h 6Eh 69h 73h 63h 68h 65h 20h 42h 75h 6Eh 64h 65h 73h 61h 6Eh 73h 74h 61h 6Ch 74h 31h 2Bh 30h 29h 06h 03h 55h 04h 0Bh 0Ch 22h 44h 61h 74h 65h 6Eh 6Bh 6Fh 6Dh 6Dh 75h 6Eh 69h 6Bh 61h 74h 69h 6Fh 6Eh 20h 90h 00h	**Antwort** Zertifikat (EF_CERT) 00 00h .. 00 7Fh Inhalt: Die ersten Byte enthalten die Längeninformation 30h: SEQUENCE 82h: Längenangabe in Byte 03h 60h: Länge des Zertifikats = 864 Byte SW1/SW2: No Error
00h B0h 00h 80h 00h 80h	**Befehl** **READ CERTIFICATE** Offset = 00 80h LC = 0 Byte LE = 80h
.. 90h 00h	**Antwort** Zertifikat 00 80h .. 00 FFh SW1/SW2: No Error
00h B0h 01h 00h 00h 80h	**Befehl** **READ CERTIFICATE** Offset = 01 00h LC = 0 Byte LE = 80h
..	
SW1/SW2=6Ah 86h (Checking error: Incorrect P1-P2) Lr=0	

* Absätze und Einzüge dienen nur der anschaulichen Darstellung

10.2 Sequenzdiagramme

10.2.1 Beispiel: Erste Initialisierung des TIM

Das folgende Beispiel zeigt den Ablauf der ersten Initialisierung. Zuerst wird mit SELECT FILE (AID) die TIM Applikation ausgewählt. Durch das folgende GET DATA TIM Status wird der Lebenszyklus überprüft, in diesem Beispiel TIM_PERSONALISED. Damit muss das TIM vor der ersten Buchung einmalig aktiviert werden. Dazu wird die Transport-PIN abgefragt. Mit dem Befehl REPORT TIM Activate wird die Transport-PIN an das TIM übergeben. Nach erfolgreicher Überprüfung gibt das TIM einen signierten Report zurück. Im Anschluss werden mit dem Befehl GET DATA TIM Status extended Informationen wie TIM-Version, Steuerpflichtigen-ID, lfd. Nummer des TIM usw. abgefragt und im Journal der Kasse abgelegt. Mit SELECT FILE (EF_CERT) wird das Zertifikat auf dem TIM ausgewählt und anschließend mit den Befehlen READ CERTIFICATE part 1..N ausgelesen. Das Zertifikat wird ebenfalls im Journal der Kasse abgelegt und später in die XML-Export-Datei(en) eingefügt.

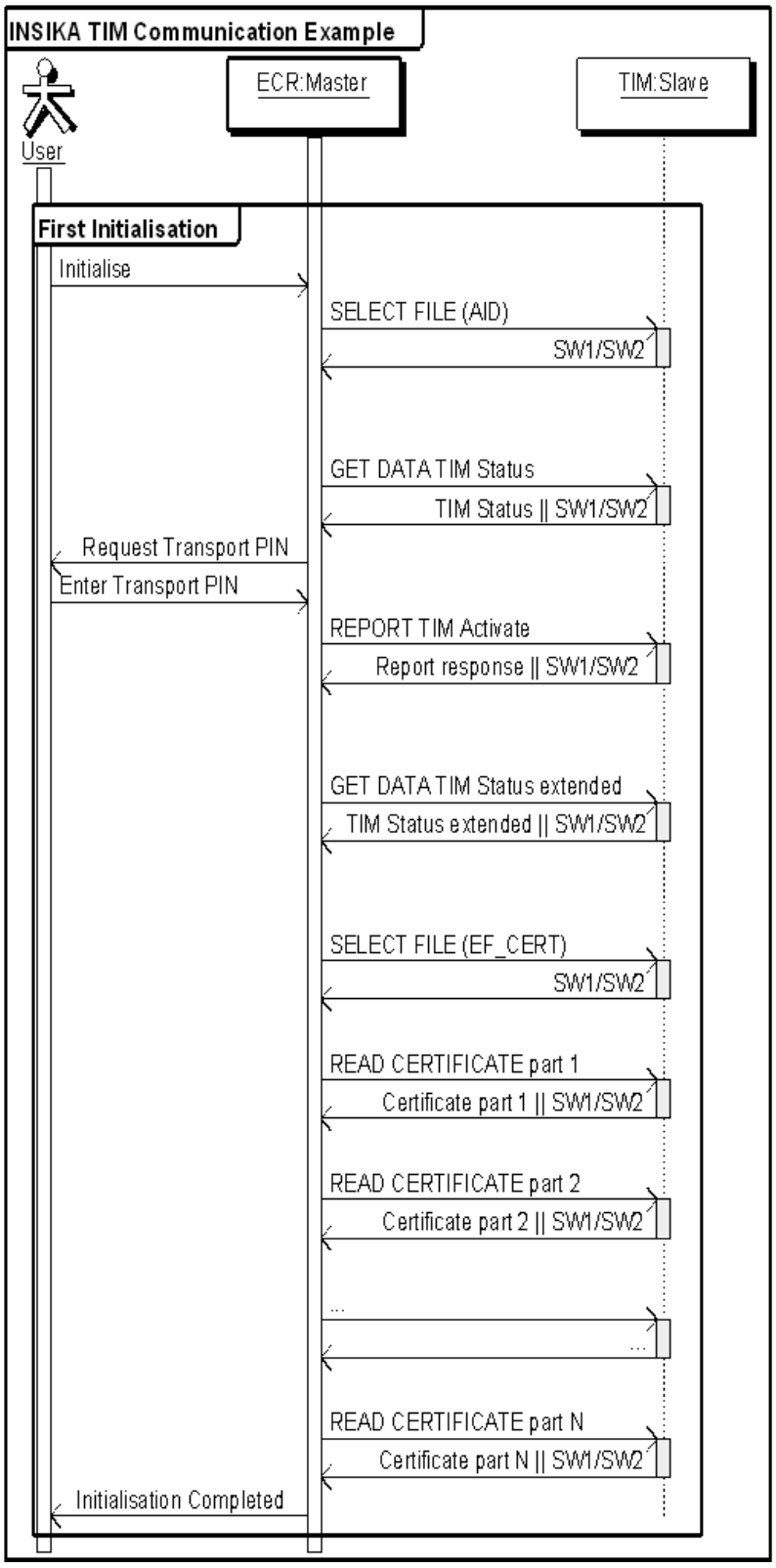

Abbildung 10-1: Sequenzdiagramm der ersten Initialisierung des TIM (Beispiel)

Anmerkung: *Der SELECT FILE (AID)-Befehl ist bei TIM ab Version V.2.0.0 nicht mehr zwingend erforderlich.*

10.2.2 Beispiel: Buchungen und Tagesabschluss

Im Folgenden wird der beispielhafte Ablauf im normalen Einsatz gezeigt. Zuerst wird die TIM-Applikation mit SELECT FILE ausgewählt. Danach werden Buchungen mit dem Befehl TRANSACTION signiert und ein Tagesabschluss mit dem Befehl REPORT signed erhalten.

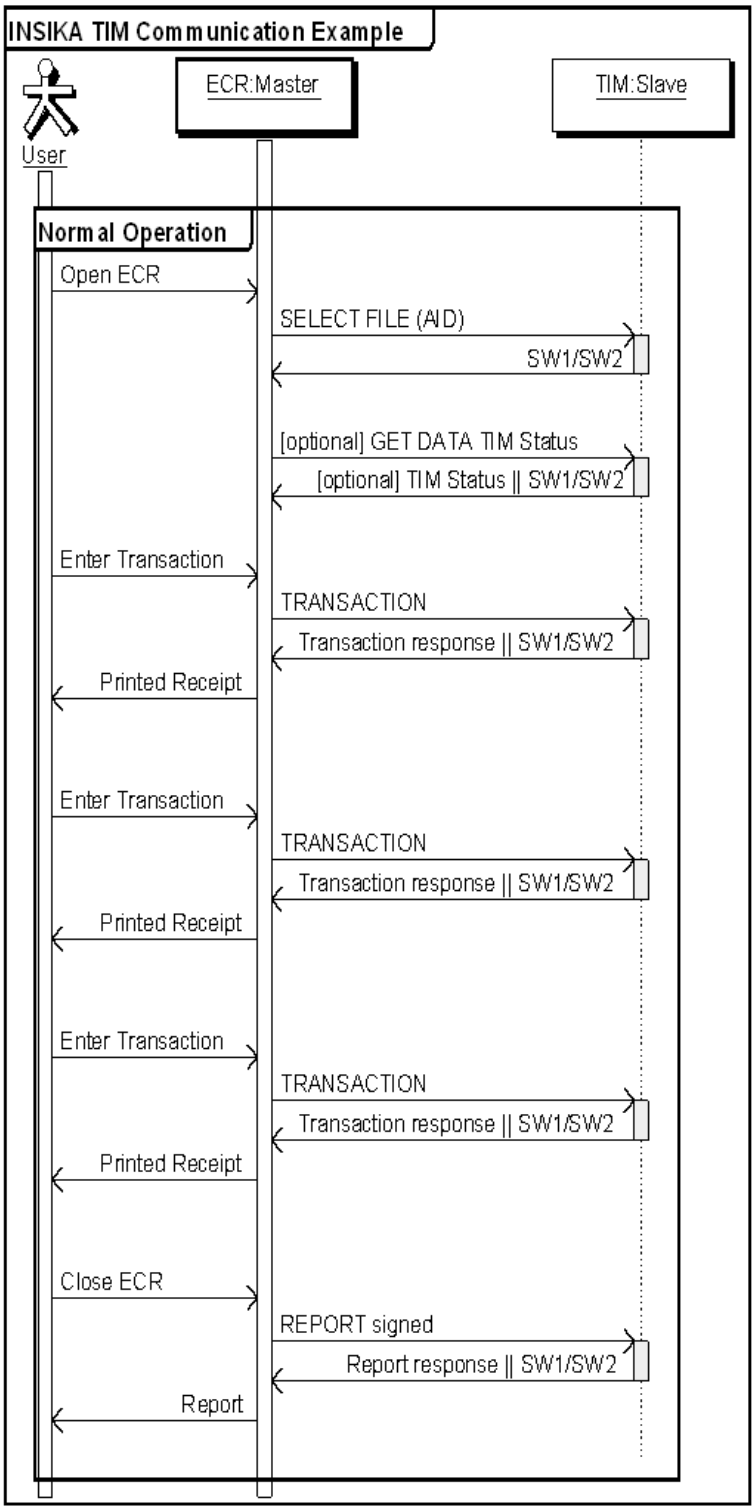

Abbildung 10-2: Sequenzdiagramm mit einem normalen Einsatz des TIM (Beispiel)

Anmerkung: *Der SELECT FILE (AID)-Befehl ist bei TIM ab Version V.2.0.0 nicht mehr zwingend erforderlich.*

10.2.3 Beispiel: Deaktivierung des TIM

Die Deaktivierung des TIM kann nur einmal vorgenommen werden. Der Befehl TRANSACTION steht danach nicht mehr zur Verfügung (siehe → 5.3). Eine erneute Aktivierung des TIM ist nicht möglich!

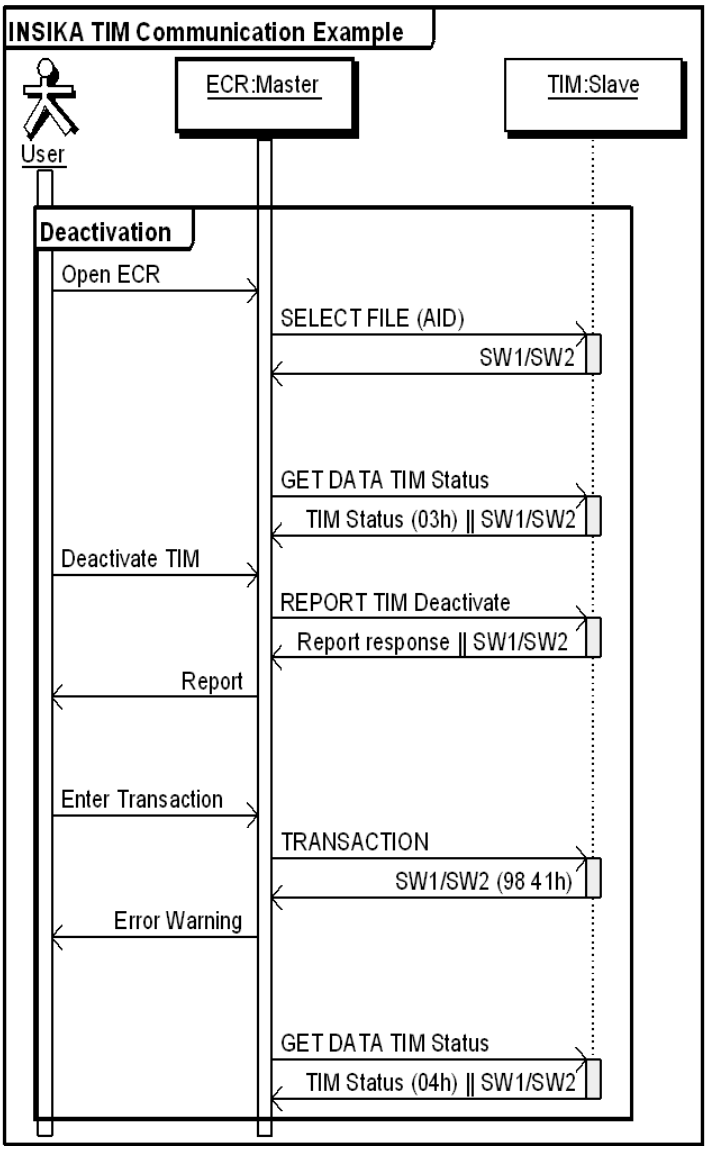

Abbildung 10-3: Sequenzdiagramm für Deaktivierung des TIM (Beispiel)

Anmerkung: *Der SELECT FILE (AID)-Befehl ist bei TIM ab Version V.2.0.0 nicht mehr zwingend erforderlich.*