INSIKA Cash Register Profile
V.2.1.0

Revision: 00

Last change: 13.03.2017

Status: released

This document is a translation of the original German version. In case of any discrepancy between the original text and this translation, the German text shall prevail.

About this document

This INSIKA documentation contains the specifications of the working group INSIKA of the ADM e.V. for the cash register profile. The publication of the documentation enables interested parties to find information on the principles of the INSIKA technology, and are thus in a position to implement the concept in practice. To be able to inform about modifications, the documentation will only be distributed to registered companies.

No guarantees or obligations can be derived from the technical contents presented in this description. The authors and the consortium assume no liability or responsibility if the concept or parts thereof are adopted and/or implemented.

In-development support for implementations is not possible. Questions about the concept will be answered as far as possible.

Further information: http://www.insika.de/

The INSIKA project was funded by the German Federal Ministry of Economics and Technology under the grant MNPQ 11/07.

Revision History

Version	Date	Change
T110-01	10.03.2015	Cash Register Profile moved from TIM specification into separate document, Documentation of 2D code added, several revisions, Review
V.2.1.0-00	13.03.2017	Publication to registered companies Changes compared to the previous version: • Alternative signature length ECDSA-256 with SHA-256 • Changes to the handling of turnovers from third party and delivery note

Authors: Jörg Wolff (PTB [until 2013])
Norbert Zisky (ADM, PTB [until 2015]))

Document:

Title:	INSIKA Cash Register Profile
Referenced TIM package:	V.2.1.0
Revision:	00
Status:	Released
Last change:	13.03.2017
File name:	INSIKA_Profile_Cash_Register-V210-00-en.docx
Number of pages:	17
Contact:	http://www.insika.de/en/contact

Table of Contents

1 General Information

1.1 Changes to previous version

Changes to the previous version result from changes of the treatment of delivery notes and third party sales. The INSIKA TIM Interface Documentation V.2.1.0 specifies the handling of deliveries or services without turnover as well as the processing of third parties sales and delivery notes.

1.2 Document information

This document describes the specific data structures, procedures and rules that must be considered when using the INSIKA system for cash registers.

It must always be used in conjunction with the document "INSIKA TIM Interface Specification" referring to the same TIM version.

1.3 Tasks, hash specification and export format

The mapping rules defined in the profiles for calculating the hash value of the transaction items (which is included in the signature of the transaction) have the task of protecting the essential data of each transaction items against tampering. From these essential data, the total turnover per tax rate of a transaction must be determined unequivocally. Each host system recording transaction data (here: each cash register) must be able to implement the hash specification.

For this reason, the hash specification never contains all the data required for complete traceability, e.g. it is not differentiated between different discount rates (absolute or percentage, based on the entire document or a position), but only the resulting discount amount (including the value-added tax allocation) is included in the hash value of the transaction items and thus in the signature of transaction..

Therefore, the data defined in the profile is usually is not sufficient for audit purposes. When using the XML export format (defined in a separate document), additional transaction data is also required. In the future there will be an export format that combines all data in one data set.

1.4 Particularities when processing turnover data

In addition to turnover from deliveries or services, this document also takes into account the handling of delivery notes and third party sales.

In the case of transaction requests to the TIM, regular sales and third party sales can be combined in one transaction, cf. INSIKA TIM Interface Documentation, V.2.1.0, 3.4.1 " Turnover plausibility Check of the TIM " and 8.2.2 " Container Third-party E7h".

Delivery notes must always be treated as a separate transaction, see above. INSIKA TIM Interface Documentation, V.2.1.0, 8.2.3. "Container Delivery Notes E8h".

2 Encoding of transaction items

The following profile serves to encode application-specific data from cash registers. As the result of this profile, the hash value of the transaction items is formed from the individual items of a transaction. This hash value is transmitted to the TIM as part of a transaction.

At a cash register, the transaction items (ITEM) are encoded in TLV objects. For this the actual data (Value) are preceded by one byte for unambiguous identification (Tag) and one byte for the length (Length). The whole data object is referred to hereinafter as TLV object.

TLV objects of type transaction item serve to image individual items of a transaction. From this, the hash value of the transaction items (→2.5) have to be formed in accordance with the hash specifications for transaction items and transmitted to the TIM as part of a transaction. TLV objects of type transaction item (prefix "ITEM") are not used in the direct communication with the TIM.

2.1 TAG (designator)

The following tags are defined for the transaction items:

Table 2-1: Summary of the defined TLV tags

Name	Tag	Description	Payload data	
			Length (Byte)	Format (→ Fehlerl Ver-
ITEM_QUANTITY	A0h	Item quantity → 2.3.1	1..16	ASCII
ITEM_UNIT	A1h	Item unit of quantity → 2.3.2	1..8	ASCII
ITEM_NAME	A2h	Item commercial designation → 2.3.3	1..16	ASCII
ITEM_DISCOUNT_SURCHARGE	AAh	Item flag discount/surcharge → 2.3.4	0	-
ITEM_VOUCHER	ABh	Item flag voucher → 2.3.4	0	-
ITEM_THIRDPARTY	ACh	item flag thirdparty→ 2.3.5	0	
ITEM_PRICE_1 … ITEM_PRICE_6	B1h … B6h	Item price 1..6 → 2.3.6	1..6	Signed BCD

2.2 LENGTH

The following encoding is used for the length:

- The length of the field (00h..7Fh) is directly encoded in one byte.

In the current version of the TIM specification, no fields with lengths longer than 127 (7Fh) are used. The BER-TLV used is therefore identical here with the "SIMPLE-TLV".

2.3 VALUE

This chapter defines the payload data to be used in the TLV objects. The following definition covers transaction items (prefix BP or ITEM).

2.3.1 BP quantity/number: ITEM_QUANTITY – A0h

The quantity or number is numerically defined and encoded as ASCII characters. The maximum permissible length is 16 characters. The decimal point is the dot. With quantities less than 1, a zero is placed in front of the decimal point. With decimal places, zeroes following the last number are omitted. Separators for thousands groups are not permitted.

The TLV object quantity/number must be indicated for every transaction item and therefore always goes into the hash value of the transaction items. The default quantity/number = 1. This applies even if the object is not printed on the sales receipt.

The TLV object quantity/number is used to image transaction items in accordance with the hash specifications (→ 2.5). It is not transmitted directly to the TIM.

Example

Examples of valid and invalid encodings:

T	L	V	Contents
A0h	01h	31h	'1'
A0h	04h	30h 2Eh 30h 34h	'0' '.' '0' '4'
A0h	03h	2Eh 30h 35h	Invalid, with quantities less than 1 a zero before the decimal sign is required
A0h	04h	31h 2Eh 32h 30h	Invalid, trailing zero must be omitted
A0h	03h	33h 37h 2Eh	Invalid, decimal point must be omitted
A0h	08h	32h 2Eh 30h 30h 30h 2Eh 38h 39h	Invalid, separators for thousands groups are not permitted

2.3.2 BP unit of quantity: ITEM_UNIT – A1h

The unit of quantity is encoded as ASCII characters with a maximum permissible length of 8 characters. If the object unit of quantity is printed on the sales receipt, it goes into the hash

value of the transaction items. If no unit of quantity is printed, the object does not go into the hash value.

The character substitution as defined in the TIM interface specification must be carried out before the hash value of the transaction items is formed. The length restriction only applies to the hash value calculation. The recorded data should contain the data in their original length.

The units of quantity for metered values must be selected by analogy with ISO 80 000. The unit of quantity consists of the unit and possibly an associated prefix.

Examples of units of quantity (before character substitution) are: "pcs", "cl", "l", "mg", "g", "kg", etc.

The TLV object unit of quantity is used to image transaction items in accordance with the hash specifications (→ 2.5). It is not transmitted directly to the TIM.

Example

T	L	V	Contents
A1h	02h	6Bh 67h	"kg"
A1h	02h	63h 6Ch	"cl"
A1h	05h	73h 74h 23h 63h 6Bh	"units"

2.3.3 BP commercial designation: ITEM_NAME – A2h

The commercial designation is encoded as ASCII characters with a maximum length of 16 characters. The commercial designation must contain at least one character; the object must not be omitted.

The character substitution as defined in the TIM interface specification must be performed before the characters of the commercial designation are entered into the hash value of the item data. After this character substitution, the length is max. 16 characters. The length restriction only applies to the hash value calculation. The recorded data should contain the data in their original length.

The TLV object commercial designation is used to image transaction items in accordance with the hash specifications (→ 2.5). It is not transmitted directly to the TIM.

Example

T	L	V	Contents
A2h	10h	66h 72h 23h 68h 73h 74h 23h 63h 6Bh 6Ch 69h 73h 73h 61h 62h 6Fh	"fr#hst#cklissabo" (formed from "Frühstück Lissabon" after character substitution)

2.3.4 BP flag discount/surcharge, voucher: ITEM_DISCOUNT_SURCHARGE – AAh ITEM_VOUCHER – ABh

Flags are encoded as TL objects without VALUE (payload data). The length field LENGTH contains the length 00h. A set flag is indicated purely by the presence of the TL object. Flags not set are not included in the calculation of the hash value of the transaction items (→ 2.5).

The flag discount/surcharge (ITEM_DISCOUNT_SURCHARGE) marks the current item as discount / surcharge. The system distinguishes between discount and surcharge using the sign of the price for this item (→ 2.3.6).

If individual goods / services are delivered free of charge in a transaction item and the reason for this is to be documented, the ITEM_DISCOUNT_SURCHARGE has to be used with a discount of 100% in an additional transaction item. The transaction item is marked as a discount / surcharge by the flag. The system distinguishes between discount and surcharge using the sign of the price for this item (→ 2.3.6).

If a discount or a surcharge is applied to the entire transaction, this has to be recorded as an additional transaction item with the flag ITEM_DISCOUNT_SURCHARGE- AAh. The discount or surcharge has to be taken into account in the transaction turnovers passed to the TIM in the transaction request. The turnovers transferred to the TIM must therefore be calculated from the transaction items.

The flag voucher (ITEM_VOUCHER) marks the current item as voucher sale / redemption. The system distinguishes between sale and redemption using the sign of the price for this item (→ 2.3.6). Down-payments are treated as vouchers.

The data model can be used to implement taxation when the voucher is issued as well as taxation when the voucher is redeemed. The choice has to made based on applicable tax law.

If taxes are due with redemption voucher must be issued and redeemed without taxes – taxes are shown together with goods and services paid for with the voucher. If taxes are due when the voucher is issued they are shown then – the redemption thus has to show negative taxes to take into account that the taxes have already been paid.

The TLV objects discount/surcharge and voucher are used to encode transaction items in accordance with the hash specifications (→ 2.5). They are not transmitted directly to the TIM.

Example

T	L	V	Contents
AAh	00h	-	Flag discount/surcharge set
ABh	00h	-	Flag Voucher set

2.3.5 ITEM Merker Agenturgeschäft: ITEM flag thirdparty ITEM_THIRDPARTY- ACh

Transaction items flagged with ITEM flag thirdparty ACh are taken over into the TIM container TIM_CONTAINER_ THIRDPARTY - E7h at transaction requests. This allows a clear separation of turnovers from regular sales from sales in the name of third parties. This is absolutely necessary for the verification of transaction data.

2.3.6 BP price 1..6: ITEM_PRICE_1..6 – B1h..B6h

The price is encoded as a signed BCD with a maximum of 11 valid digits. The data type "signed BCD" is defined in the TIM interface specification. Leading zero bytes must be suppressed. Prices with the value zero are not included in the forming of the hash.

The data field Price shows the total price of the individual transaction items (i.e. price = quantity/number x unit price). The price is shown without decimal point in the small currency unit (Euro Cents). If necessary, the price must be rounded to whole Cents according to commercial principles. With metered values, the unit price of a transaction item can be determined from the quantity, unit of quantity and the total price of the item.

The corresponding price 1..6 has to be selected, depending on the VAT rate. The assignment is defined in section → 2.4.

A transaction item may contain several price components (e.g. B1h price 1 and B2h price 2). This allows products to have different VAT rates for different components.

The TLV objects Price 1..6 are used to encode transaction items in accordance with the hash specifications (→ 2.5). They are not transmitted directly to the TIM.

Examples of valid and invalid encodings (here for Euro amounts):

T	L	V	Contents
B1h	02h	12h 3Ch	Price 1: 1.23 €
B2h	03h	01h 23h 4Dh	Price 2: -12.34 €
B4h	01h	1Ch	Price 4: 0.01 €
B1h	04	01h 00h 00h 0Ch	Price 1: 1000.00 €
B1h	06h	00h 00h 00h 00h 12h 3Ch	**Invalid**, leading zero bytes not suppressed
B2h	03h	34h 56h 70h	**Invalid** sign
B1h	01h	0Ch	**Invalid**, value zero is not included in the hash
B1h	01h	0Dh	**Invalid** sign for zero

2.4 Definition of the BP Price 1..6

Six different prices are defined, depending on the VAT class. The definition of the transaction items Prices 1..6 in Table 2-2: Definition of prices 1..6 in accordance with the VAT classes follows the specifications for the VAT classes for containers 1..6 (→ TIM interface specification).

Table 2-2: Definition of prices 1..6 in accordance with the VAT classes

Name	Tag	Designation of VAT class	Designation and VAT rate in Germany (2015)
ITEM_PRICE_1	B1h	Standard	Standard rate: 19%
ITEM_PRICE_2	B2h	Reduced 1	Reduced rate 7%
ITEM_PRICE_3	B3h	Reduced 2	Does not exist
ITEM_PRICE_4	B4h	VATfree	0%
ITEM_PRICE_5	B5h	Special 1	Average rate 1: 10.7%
ITEM_PRICE_6	B6h	Special 2	Average rate 2: 5.5%

2.5 Hash Specification for Transaction Items

This specification defines the content and order of the TLV objects into which the item data of a transaction have to be converted. The hash value of the transaction items is formed over these TLV objects with SHA-1/SHA-256[1]. This hash value of the transaction items is transmitted to the TIM as part of a transaction and signed together with this transaction.

[1] When applying for INSIKA cards, the cryptographic algorithms can be chosen. It has to be determined whether the card is to work a) with ECDSA-192 / SHA-1 (value above) or b) with ECDSA-256 / SHA-256 (value below). For the new card generation variant b) is the default configuration:

Table 2-3: Hash specification for the transaction items

Tag	Length (Byte)			possi-bly not trans-mitted[2]	Order
A0h	1..16	Item 1	quantity/number		1
A1h	1..8		unit of quantity	X	2
A2h	1..16		commercial designation		3
AAh	0		discount / surcharge	X	4
ABh	0		voucher	X	5
ACh	0		thirdparty	X	6
B1h … B6h	1..6 … 1..6		price 1 … price 6	X	7 ... 12
⋮					
A0h	1..16	Item n	quantity/number		
A1h	1..8		unit of quantity	X	
A2h	1..16		commercial designation		
AAh	0		discount / surcharge	X	
ABh	0		voucher	X	
ACh	0		thirdparty	X	
B1h … B6h	1..6 … 1..6		price 1 … price 6	X	

The individual transaction items are not separated from one another by a special tag. The order of the individual transaction items must be identical to the order on the printed document!

[2] The corresponding TLV objects must be omitted and not included in the formation of the hash:
- If unit of quantity is not printed
- No flag set
- Price = 0

3 Reports (Daily closing)

The cash register profile does not specify any additional report items for the daily closing. Thus the REPORT command is used without the optional hash value.

4 Verification of receipts

4.1 Printed receipts (plain text)

Requirements for printing receipts:

- The Signature has to be printed in Base32 encoding. To improve legibility it must be formatted in groups of five characters each. These groups can be separated by spaces or dashes.
- The hash value over the transaction items is printed in the same style as the signature.
- Text has to printed in a way, that after character substitution (according to TIM specification) stored and printed data are identical.
- It must be obvious from the printed transaction items how the TLV objects defined in section 2 are created. This includes the requirement that the order in the printout is exactly identical to the order of the objects during calculation of the hash value.

4.2 QR-Codes

Remark: This description is preliminary! At the least the URL of the verification server will change in a live system.

The content of the 2D code is a URL that contains the name of the verification server and a parameter t1 (for "transaction, version 1") which consists of the Base64 encoded elements of the TRANSACTION request and the positive answer returned by the TIM.

Example (in 192 bit mode only):

Data to TIM:

```
CD0420100422CE021513C6086963686E69636874C71453E0D325EFA04689EEC6A20C
D02DC824E781DBECE107D802105CDB0100
```

Answer of TIM:

```
C410494E53494B412D544553545F5054426AC50101CB01019E302BAA3E195A19FDFE
926FC0430FBEAE4CF615A3434366150DC20E764743FB13A841D89F1AB08C1E5D54BF
D69E63C8A361
```

Base64-encoded:

```
zQQgEAQizgIVE8YIaWNobmljaHTHFFPg0yXvoEaJ7saiDNAtyCTngdvs4QfYAhBc2wEA
xBBJTlNJS0EtVEVTVF9QVEJqxQEBywEBnjArqj4Zwhn9/pJvwEMPvq5M9hWjQ0NmFQ3C
DnZHQ/sTqEHYnxqwjB5dVL/WnmPIo2E=
```

According to RFC 2396 not all of the characters may be used. Thus "/" and "+" have to be substituted (http://tools.ietf.org/html/rfc2396):

```
3.4. Query Component
```

```
The query component is a string of information to be interpreted by
the resource.
query         = *uric
 Within a query component, the characters ";", "/", "?", ":", "@",
"&", "=", "+", ",", and "$" are reserved.
```

The alternative Base64 encoding proposed in RFC 3548 (Base64 Encoding with URL and Filename Safe Alphabet) is used. Accordingly the characters “+” and “/” are replaced with “-“ and “_” (http://tools.ietf.org/html/rfc3548).

The above example now looks like this:

```
zQQgEAQizgIVE8YIaWNobmljaHTHFFPg0yXvoEaJ7saiDNAtyCTngdvs4QfYAhBc2wEA
xBBJTlNJS0EtVEVTVF9QVEJqxQEBywEBnjArqj4ZWhn9_pJvwEMPvq5M9hWjQ0NmFQ3C
DnZHQ_sTqEHYnxqwjB5dVL_WnmPIo2E=
```

This leads to the following URL which will be encoded in the QR code:

```
http://insika.de/verify.php?t1=zQQgEAQizgIVE8YIaWNobmljaHTHFFPg0yXvo
EaJ7saiDNAtyCTngdvs4QfYAhBc2wEAxBBJTlNJS0EtVEVTVF9QVEJqxQEBywEBnjArq
j4ZWhn9_pJvwEMPvq5M9hWjQ0NmFQ3CDnZHQ_sTqEHYnxqwjB5dVL_WnmPIo2E=
```

Due to the Base64 encoding one or more “=” characters can be added to the data. They must not be cut off!

Example for a receipt with QR Code

Generated by KassSim.exe demo software.

Item hash and signature are not only included in the QR code, they are also printed as text in Base32 encoding.

```
              PTB-DEMO-Kasse
Gurke                         B          1,49€
Linseneintopf                 B          0,69€
Makrelenfilet                 B          2,39€
Pfandartik.Einweg             A          0,25€
-------------------------------------------------
Summe                                    4,82€

Steuer%  Brutto    Netto      Steuer
A  19.0  0,25€     0,21€      0,04€
B  7.00  4,57€     4,27€      0,30€

Hash BP
BQ6BJ-3FT3M-7F70S-RZPJB-ZYYJ6-D23R0-32
Signatur
6SGHI-2P434-7GW7D-BSG3M-WRFZ7-LJPH7-
JVSER-J2VQ5-AV76L-XVCZA-S60SJ-FZM0I-
3GTIG-ZZMCC-KNE66-TK=

Datum:                2010-07-27
Zeit:          09:50
Bediener-ID:  ICHnicht
Steuerpfl.ID:         INSIKA_TEST_PTB
Steuerpfl.ID Nr: 2
Seq.Nr. Buchung: 135
```

The QR code contains the following link:

http://insika.de/verify.php?t1=zQQgEAcnzgIJUMYIaWNobmljaHTHFAw8FOyz2z5fulHL0hzjCfD1uLt64QjYAgJc2wIZAOII2AJFfNsCBwDED0lOU0lLQV9URVNUX1BUQsUBAssBh54w9Ix0afzfPmt8YZG2y0S5-tLz_TWRIp1WHQV_5d6iyCXnSSXLHI2aaDZywQlNJ701

The **Google Chart API** can be used as an example for QR-Code generation: https://google-developers.appspot.com/chart/infographics/docs/overview

Example:

http://chart.googleapis.com/chart?chs=200x200&cht=qr&chl=http://insika.de/verify.php?t1=zQQgEAcnzgIJUMYIaWNobmljaHTH-FAw8FOyz2z5fulHL0hzjCfD1uLt64QjYAgJc2wIZAOII2AJFfNsCBwDED0lOU0lLQV9URVNUX1BUQsUBAssBh54w9Ix0afzfPmt8YZG2y0S5-tLz_TWRIp1WHQV_5d6iyCXnSSXLHI2aaDZywQlNJ701