GS1 Switzerland

The Global Language of Business

EDI – Ideal Message CH INVOIC

Security Segments

Overview

Document information	
Title	Ideal Message INVOIC - Security Segments - Vers. 3.5.0
Last modification	December 2022
Version	3.5.0 Based on EANCOM ® 2002
Publication	December 2022
Publisher	GS1 Switzerland
Image source	iStock

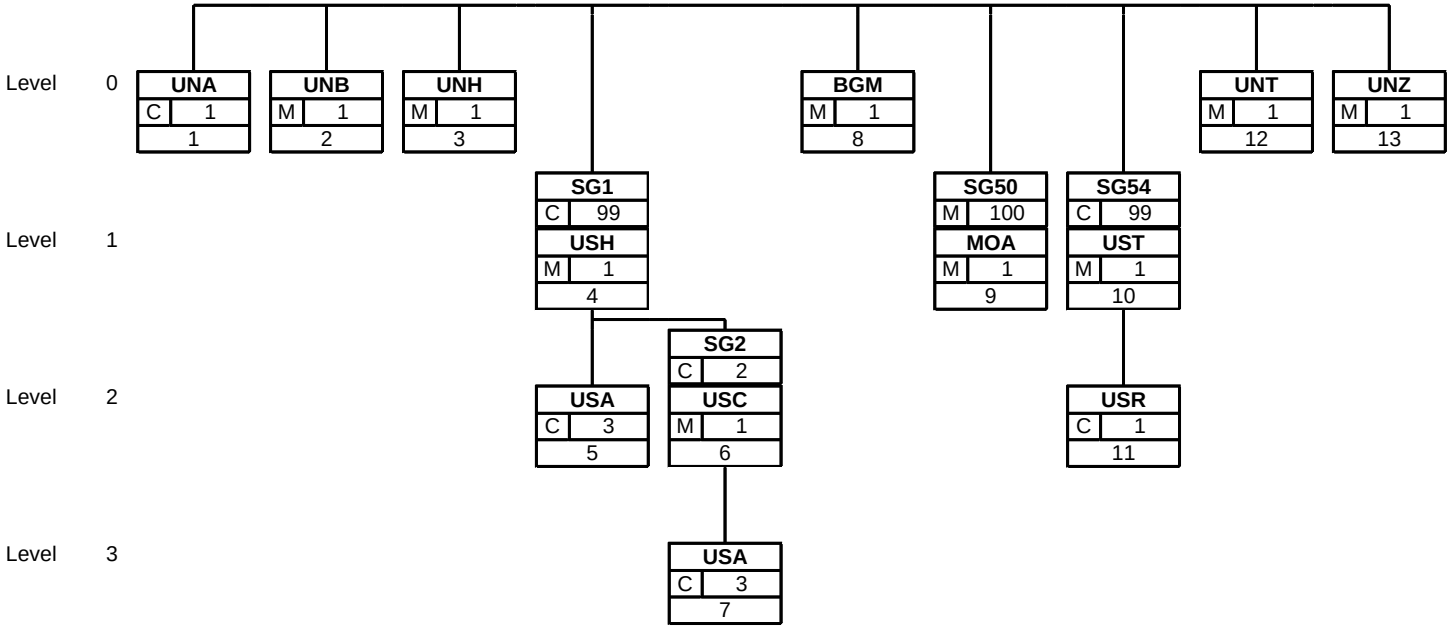
Disclaimer

INVOIC

Meldungsbeschreibung

In diesem Dokument sind die Security-Elemente der elektronsichen INVOIC beschrieben.
Die genaue Platzierung der einzelnen Sicherheitselemente sind im Branching-Diagramm dargestellt.

INVOIC - Branching Diagram



INVOIC

Segment: **UNA** lfd. Nr.: 1 Ebene: 0 **Service string advice**
Status: C Max. Wdh.: 1

Beschreibung: **Service string advice**

Formale Beschreibung des Segments:

EDIFACT			Anwendung		
	Beschreibung	St Format	St	Beispiel	Verwendung / Hinweise
UNA1	Component data element separator	M an1	M*	:	Trennzeichen der Felder innerhalb einer Segmentgruppe Used as a separator between component data elements contained within a composite data element (value ":").
UNA2	Data element separator	M an1	M*	+	Trennzeichen der Segmentgruppen innerhalb eines Segmentes Used to separate two simple or composite data elements (value: "+").
UNA3	Decimal mark	M an1	M*	.	Dezimaltrennzeichen Used to indicate the character used for decimal notation (value: ".").
UNA4	Release character	M an1	M*	?	Freigabezeichen Used to restore any service character to its original specification (value: "?").
UNA5	Repetition separator	M an1	M*	*	Repetitionszeichen Used to indicate the character used for repetition separation (value: " * ").
UNA6	Segment terminator	M an1	M*	'	Segment-Endzeichen Used to indicate the end of segment data (value: " ' ").

Kommentar EANCOM:
This segment is used to inform the receiver of the interchange about the set of service characters (and decimal mark) which are being used.
It must immediately precede the UNB segment and contains the five service characters (positions UNA1, UNA2, UNA4, UNA5 and UNA6) selected by the interchange sender.
When expressing the service characters in the UNA segment, it is not necessary to include any element separators.
Within EANCOM®, using the default set of service characters, the use of the UNA segment is not required.

Beispiel:
UNA:+.?*'

INVOIC

Segment: **UNB** lfd. Nr.: 2 Ebene: 0 **Interchange header**
Status: M Max. Wdh.: 1

Beschreibung: **Interchange header**

Formale Beschreibung des Segments:

EDIFACT				Anwendung		
	Beschreibung	St	Format	St	Beispiel	Verwendung / Hinweise
S001	Syntax identifier	M		M		See Part I chapter 5.2.7 and segment notes.
0001	Syntax identifier	M	a4	M*	+UNOC	**UNOC UN/ECE level C** UNOC erlaubt Gross-/Kleinschrift, Sonderzeichen und Umlaute The recommended (default) character set for use in EANCOM® for international exchanges is character set A (UNOA). Should users wish to use character sets other than A, an agreement on which set to use should be reached on a bilateral basis before communications begin.
0002	Syntax version number	M	an1	M*	:4	**4 Version 4**
S002	Interchange sender	M		M		
0004	Interchange sender identification	M	an..35	M	+5412345 678908	GLN (n13) Within EANCOM® the use of the Global Location Number (GLN) is recommended for the identification of the interchange sender and recipient.
0007	Identification code qualifier	C	an..4	R*	:14	**14 EAN International**
0008	Interchange sender internal identification	C	an..35	O	: 541234567 8939	GLN der internen Rückmeldungsadresse des Senders Within EANCOM® the use of the Global Location Number (GLN) is recommended for the identification of the interchange sender and recipient. Identification (e.g. a division) specified by the sender of the interchange, to be included if agreed, by the recipient in response interchanges, to facilitate internal routing.
S003	Interchange recipient	M		M		
0010	Interchange recipient identification	M	an..35	M	+8798765 432106	GLN des Nachrichten-Empfängers GLN (n13) Within EANCOM® the use of the Global Location Number (GLN) is recommended for the identification of the interchange sender and recipient.
0007	Identification code qualifier	C	an..4	R*	:14	**14 EAN International**
0014	Interchange recipient internal identification	C	an..35	O	: 879876543 2151	GLN der internen Weiterleitungsadresse des Empfängers Within EANCOM® the use of the Global Location Number (GLN) is recommended for the identification of the interchange sender and recipient.
S004	Date and time of preparation	M		M		
0017	Date	M	n8	M	+2006011 0	CCYYMMDD
0019	Time	M	n4	M	:1015	HHMM
0020	Interchange control reference	M	an..14	M	+1234555 5	Unique reference identifying the interchange. Created by the interchange sender.
S005	Recipient reference/password details	C		N		
0022	Recipient reference/password	M	an..14	N	+	
0026	Application reference	C	an..14	O	+	Message identification if the interchange contains only one type of message. This data element is used to identify the application, on the interchange recipient's system, to which the interchange is directed. This data element may only be used if the interchange contains only one type of message, (e.g. only

INVOIC

EDIFACT			Anwendung		
	Beschreibung	St Format	St	Beispiel	Verwendung / Hinweise
					invoices). The reference used in this data element is assigned by the interchange sender.
0029	Processing priority code	C a1	N	+	
0031	Acknowledgement request	C n1	O	+1	**1 Requested** This data element is used to indicate whether an acknowledgement to the interchange is required. The EANCOM® APERAK or CONTRL message should be used to provide acknowledgement of interchange receipt. In addition, the EANCOM® CONTRL message may be used to indicate when an interchange has been rejected due to syntax errors.
0032	Interchange agreement identifier	C an..35	O*	+EANCOM REF 52	EANCOM..... This data element is used to identify any underlying agreements which control the exchange of data. Within EANCOM® , the identity of such agreements must start with the letters 'EANCOM', the remaining characters within the data element being filled according to bilateral agreements.
0035	Test indicator	C n1	O	+1'	**1 Interchange is a test**

Kommentar
This segment is used to envelope the interchange, as well as to identify both, the party to whom the interchange is sent and the party who has sent the interchange. The principle of the UNB segment is the same as a physical envelope which covers one or more letters or documents, and which details, both the address where delivery is to take place and the address from where the envelope has come.

Beispiel INVOIC:

UNB+UNOC:4+5412345678908:14:5412345678939+8798765432106:14:8798765432151+20060110:1015+12345555+12345++++EANCOMREF 52'

Beispiel INVOIC-BELA:

Um die Datei als "Belastungsanzeige" zu identifizieren, ist in DE UNB_0022 die Angabe REK erforderlich:UNB+UNOC:4+7610000000000:14+7611000000000:14+201217:1302+4905+REK'

INVOIC

Gruppe: SG1; 01; CH Status: C Max. Wdh.: 99 USH-USA-SG2

Segment: USH lfd. Nr.: 4 Ebene: 1 **Security header**
Status: M Max. Wdh.: 1

Beschreibung: **Security header**

Formale Beschreibung des Segments:

EDIFACT				Anwendung		
	Beschreibung	St Format	St	Beispiel	Verwendung / Hinweise	
0501	Security service, coded	M an..3	M*	+1	**1** **5** 1 = Regelfall 5 = Falls Autack notwendig	**Non-repudiation of origin** **Non-repudiation of receipt**
0534	Security reference number	M an..14	M	+123456789	Message Reference number Beispiel 123456789	
0541	Scope of security application, coded	C an..3	R*	+1	**1**	**Security header and message body**
0503	Response type, coded	C an..3	R*	+1	**1** **2** 2 = falls Autack (Hinweis nur bei Daten gem. Art 3. Abs 2. EIDI-V (self Billing, Gutschriftserteilung) ist der AUTACK zwingend.)	**No Acknowledgement required** **Acknowledgement required**
0505	Filter function, coded	C an..3	R*	+6	**2** **5** **6**	**Hexadecimal filter** **UN/EDIFACT EDA filter** **UN/EDIFACT EDC filter**
0507	Original character set encoding, coded	C an..3	R*	+2	**2**	**ASCII 8 bit**
0509	Role of security provider, coded	C an..3	O	+1	**1** **2** **3** **4** **ZZZ**	**Issuer** **Notary** **Contracting party** **Witness** **Mutually agreed**
S500	Security identification details	C	N			
0577	Security party qualifier	M an..3	N	+		
S500	Security identification details	C	C			
0577	Security party qualifier	M an..3	N	+		
0520	Security sequence number	C an..35	N	+		
S501	Security date and time	C	R			
0517	Date and time qualifier	M an..3	R*	+1	**1**	**Security Timestamp**
0338	Event date	C n..8	R	:20050719	Format is CCYYMMDD, UTC Date. Note: UTC is alos known as GMT (Greenwich Mean Time) Beispiel 20050719	
0314	Event time	C an..15	R	:112000'	Format is CCYYMMDD, UTC Date. Note: UTC is also known as GMT (Greenwich Mean Time) Beispiel 112000	

Kommentar EANCOM:
A segment specifying a security service applied to the referenced EDIFACT structure. A Security service data element (DE 0501) shall specify the security service applied to the referenced EDIFACT structure.

Beispiel:
USH+1+123456789+1+1+6+2+1++++1:20050719:112000'

INVOIC

Gruppe: **SG1; 01; CH** Status: C Max. Wdh.: 99 USH-USA-SG2

Segment: **USA** lfd. Nr.: 5 Ebene: 2 **Security algorithm**
Status: C Max. Wdh.: 3

Beschreibung: **Security algorithm**

Formale Beschreibung des Segments:

EDIFACT				Anwendung			
	Beschreibung	St	Format	St	Beispiel	Verwendung / Hinweise	
S502	Security algorithm	M		M			
0523	Use of algorithm, coded	M	an..3	M*	+1	**1**	**Owner hashing**
0525	Cryptographic mode of operation, coded	C	an..3	N	:		
0533	Mode of operation code list identifier	C	an..3	N	:		
0527	Algorithm, coded	C	an..3	R*	:16	**16**	**SHA1**
0529	Algorithm code list identifier	C	an..3	R*	:1'	**1**	**UN/CEFACT**

Kommentar EANCOM:
This segment is used to identify a security algorithm, the technical usage made of it, and contains the technical parameters required in order to generate the hash value. At least one occurrence of this segment is mandatory.

Beispiel:
USA+1:::16:1'

INVOIC

Gruppe: **SG1; 01; CH** Status: C Max. Wdh.: 99 USH-USA-SG2

Gruppe: **SG2; 01; CH** Status: C Max. Wdh.: 2 USC-USA

Segment: **USC** lfd. Nr.: 6 Status: M Ebene: 2 Max. Wdh.: 1 **Certificate**

Beschreibung: **Certificate**

Formale Beschreibung des Segments:

EDIFACT				Anwendung		
	Beschreibung	St	Format	St	Beispiel	Verwendung / Hinweise
0536	Certificate reference	C	an..35	C	+12345	Hexadezimale Darstellung von Integer
S500	Security identification details	C		R		Das erste S500 mit Codewert 4 im 0577 ist mandatory, das zweite mit Codewert 3 im 0577 ist optional!
0577	Security party qualifier	M	an..3	M*	+4	**4 Authenticating party** 4 = Regelfall
0538	Key name	C	an..35	N	:	
0511	Security party identification	C	an..512	R	:Abc	Encoded DER encoded issuer Distinguished name (DN) of the CA - note 2
S500	Security identification details	C		O		
0577	Security party qualifier	M	an..3	M*	*3	**3 Certificate owner**
0538	Key name	C	an..35	N	:	
0511	Security party identification	C	an..512	C	:Def'	Encoded DER subject Distinguished name (DN)

Kommentar EANCOM:
Note 1: Since the full certificate is not exchanged within this message, the used certificate is identified by its reference's number in DE0536 and in the first repetition of DE S500, with the security identification details of the Certification Authority. Optionally, the encoded DER encoded subject DN can be supplied in the second repetition of DE S500
Note2:To encode either EDA-Filter, EDC-Filter or HEX-Filter has to be used as stated in UHS 0505.

Beispiel:
USC+12345+4::Abc*3::Def'

INVOIC

Gruppe: SG1; 01; CH Status: C Max. Wdh.: 99 USH-USA-SG2

Gruppe: SG2; 01; CH Status: C Max. Wdh.: 2 USC-USA

Segment: USA lfd. Nr.: 7 Status: C Ebene: 3 Max. Wdh.: 3 **Security algorithm**

Beschreibung: **Security algorithm**

Formale Beschreibung des Segments:

EDIFACT				Anwendung		
	Beschreibung	St	Format	St	Beispiel	Verwendung / Hinweise
S502	Security algorithm	M		M		
0523	Use of algorithm, coded	M	an..3	R*	+6	**6** **Owner signing**
0525	Cryptographic mode of operation, coded	C	an..3	R*	:16	**16** **DSMR**
0533	Mode of operation code list identifier	C	an..3	R*	:1	**1** **UN/CEFACT**
0527	Algorithm, coded	C	an..3	R*	:10	**10** **RSA**
0529	Algorithm code list identifier	C	an..3	R*	:1	**1** **UN/CEFACT**
0591	Padding mechanism, coded	C	an..3	R*	:16	**11** **PKCS #1 signature padding** **16** **RSASA-PKCS-v1_5** Offizielle und richtige Bezeichnung ist: RSASSA-PKCS-v1_5. In der EDIFACT Codeliste falsch bezeichnet. Aus Sicht Sicherheitsexperte Schweiz sind 11 und 16 identisch: ... and RSASSA-PKCS1-v1_5 (Section 8.2) have traditionally been employed together without any known bad interactions (indeed, this is the model introduced by PKCS #1 v1.5).
0601	Padding mechanism code list identifier	C	an..3	R*	:1'	**1** **UN/CEFACT**

Kommentar EANCOM:
This segment is used to identify the security algorithm the technical usage made of it, and contains the technical parameters required in order to generate the digital signature.

Beispiel:
USA+6:16:1:10:1:16:1'

INVOIC

Gruppe: **SG54; 01; CH** Status: C Max. Wdh.: 99 UST-USR

Segment: **UST** lfd. Nr.: 10 Ebene: 1 **Security trailer**
Status: M Max. Wdh.: 1

Beschreibung: **Security trailer**

Formale Beschreibung des Segments:

EDIFACT			Anwendung		
	Beschreibung	St Format	St	Beispiel	Verwendung / Hinweise
0534	Security reference number	M an..14	M	+123456789	Contains a number which links the validation results to the corresponding USH segment (DE0534) using the security functions. 123456789
0588	Number of security segments	M n..10	M	+6'	The number of security segments in a security header/ trailer group pair. Only the segment goups 1, 2 and 4 are counted. Each security header/trailer group pair shall contain its own count of the number of security segments within that group pair.

Kommentar EANCOM:
A segment established a link between security header and security trailer segment group, and stating the number of securitys segments in these groups.

Beispiel:
UST+123456789+6'

INVOIC

Gruppe: **SG54; 01; CH** Status: C Max. Wdh.: 99 UST-USR

Segment: **USR** lfd. Nr.: 11 Ebene: 2 **Security result**
Status: C Max. Wdh.: 1

Beschreibung: **Security result**

Formale Beschreibung des Segments:

EDIFACT				Anwendung		
	Beschreibung	St	Format	St	Beispiel	Verwendung / Hinweise
S508	Validation result	M		M		
0563	Validation value, qualifier	M	an..3	M*	+1	**1 Unique validation value**
0560	Validation value	C	an..512	R	:X'	Digital signature Hex Darstellung vom Binär Wert siehe USH 505

Kommentar EANCOM:
A segment containing the result of the security functions applied to the message package as specified in the linked security header group (as defined in Part 5 of ISO 9735).

Beispiel:
USR+1:X'

INVOIC

Segment: **UNZ** lfd. Nr.: 13 Status: M Ebene: 0 Max. Wdh.: 1 **Interchange trailer**

Beschreibung: **Interchange trailer**

Formale Beschreibung des Segments:

EDIFACT				Anwendung	
	Beschreibung	St Format	St	Beispiel	Verwendung / Hinweise
0036	Interchange control count	M n..6	M	+1	Number of messages or functional groups within an interchange.
0020	Interchange control reference	M an..14	M	+12345555'	Identical to DE 0020 in UNB segment.

Kommentar EANCOM:
This segment is used to provide the trailer of an interchange.

Beispiel:
UNZ+1+12345555'

GS1 Switzerland – The Global Language of Business

Global Standards provide more efficiency in value networks. GS1 Switzerland supports companies in optimizing their flows of goods, information and values and provides practical knowledge. Together with our members, we develop standards and process recommendations and create benefits for all parties involved. GS1 Switzerland is a neutral association based in Bern and part of the not-for-profit organization GS1, which is active in 140 countries.

GS1 Switzerland
Monbijoustrasse 68
CH-3007 Bern
T +41 58 800 70 00
www.gs1.ch