EANCOM® 2002 S4

AUTACK

Secure authentication and acknowledgement message

Edition 2016 Upd. 2021

1. Introduction

Status

MESSAGE TYPE	:AUTACK
REFERENCE DIRECTORY	:D.01B
EANCOM® SUBSET VERSION	:001

Definition

The service message AUTACK (Secure Authentication and Acknowledgement Message) enables the transmission of integrity and authenticity data for referenced data. The message is used to transport the digital signature and the related information needed by the recipient to verify the digital signature.

The secure authentication and acknowledgement message (AUTACK) may be used for both national and international trade. It is based on universal practice related to administration, commerce and transport, and is not dependent on the type of business or industry.

Principles

The applied security procedures shall be agreed to by trading partners and specified in an interchange agreement. The secure authentication and acknowledgement message (AUTACK) applies security services to other EDIFACT structures (messages, packages, groups or interchanges). It can be applied to combinations of EDIFACT structures that need to be secured between two parties.

The security services are provided by cryptographic mechanisms applied to the content of the original EDIFACT structures. The results of these mechanisms form the body of the AUTACK message, supplemented by relevant data such as references to the cryptographic methods used, the reference numbers for the EDIFACT structures and the date and time of the original structures.

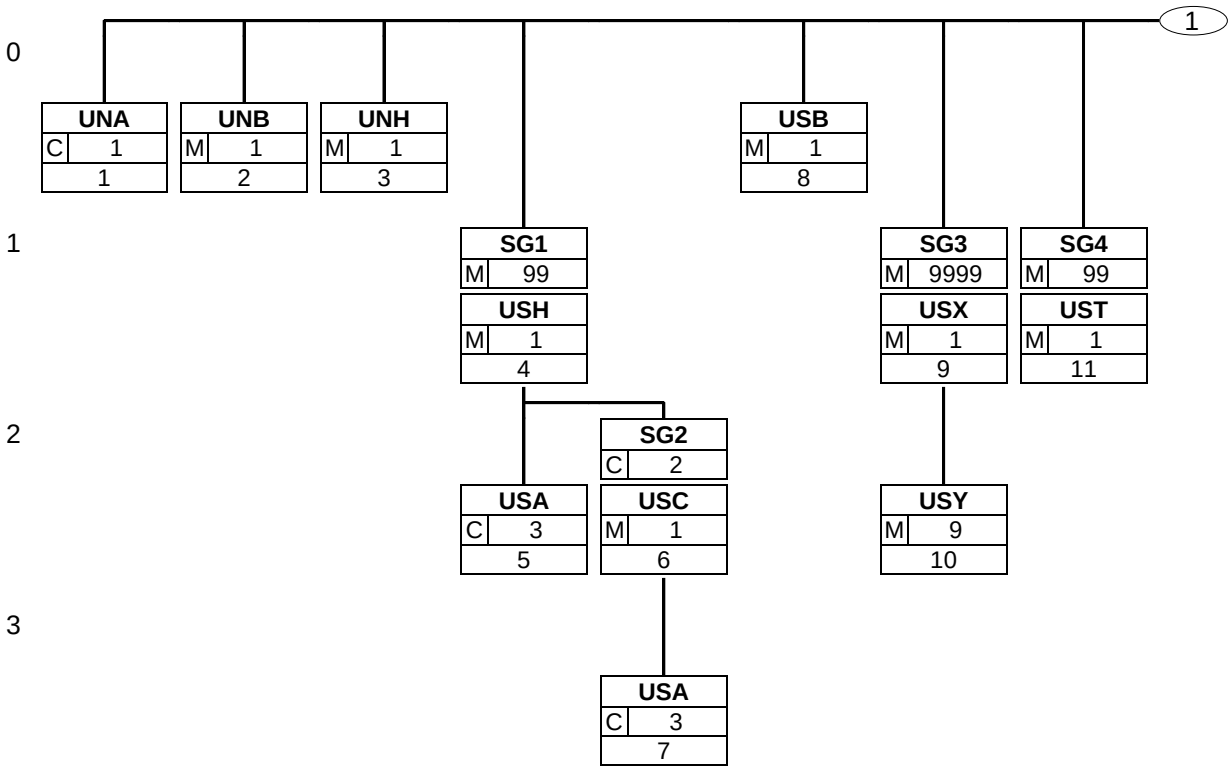
The AUTACK message can apply to one or more messages, packages or groups from one or more interchanges.

An AUTACK message used as an authentication message shall be sent by the originator of one or more other EDIFACT structures, or by a party having authority to act on behalf of the originator. Its purpose is to facilitate the security services provided by electronic signatures, i.e., authenticity, integrity, and non-repudiation of origin of its associated EDIFACT structures.

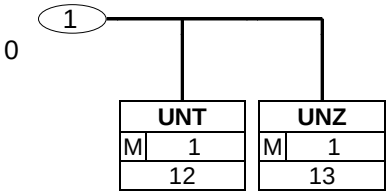
2. Message Structure Chart

UNA	1	C	1	- Service string advice
UNB	2	M	1	- Interchange header
UNH	3	M	1	- Message header
SG1		M	99	- USH-USA-SG2
USH	4	M	1	- Security header
USA	5	C	3	- Security algorithm
SG2		C	2	- USC-USA
USC	6	M	1	- Certificate
USA	7	C	3	- Security algorithm
USB	8	M	1	- Secured data identification
SG3		M	9999	- USX-USY
USX	9	M	1	- Security references
USY	10	M	9	- Security on references
SG4		M	99	- UST
UST	11	M	1	- Security trailer
UNT	12	M	1	- Message trailer
UNZ	13	M	1	- Interchange trailer

3. Branching Diagram



3. Branching Diagram



4. Segments Description

UNA - C 1 - Service string advice

This segment is used to inform the receiver of the interchange that a set of service string characters which are different to the default characters are being used.

UNB - M 1 - Interchange header

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.

UNH - M 1 - Message header

This segment is used to head, identify and specify a message.

SG1 - M 99 - **USH-USA-SG2**

A group of segments identifying the security service and security mechanisms applied and containing the data necessary to carry out the validation calculations. This segment group shall specify the security service and algorithm(s) applied to the referenced EDIFACT structure. Each security header group shall be linked to a security trailer group, and additionally linked to the USY segment(s).

USH - M 1 - Security header

A segment specifying a security service applied to the referenced EDIFACT structure.

USA - C 3 - Security algorithm

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.

SG2 - C 2 - **USC-USA**

A group of segments containing the data necessary to validate the security methods applied.

USC - M 1 - Certificate

This segment either contains information regarding the certificate, and identifies the certification authority which has generated the certificate, or is used to identify bilaterally interchanged signature keys.

USA - C 3 - Security algorithm

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 digital signature.

USB - M 1 - Secured data identification

This segment shall contain identification of the interchange sender and interchange recipient.

SG3 - M 9999 - **USX-USY**

This segment group shall be used to identify a party in the security process and to give security information for the referenced EDIFACT structure.

USX - M 1 - Security references

This segment shall contain references to EDIFACT structures (i.e., interchanges, groups or messages) to which security services were applied.

USY - M 9 - Security on references

This segment contains a link to the security header group and the result of the security services applied to the referenced EDIFACT structure (i.e., the digital signature) as specified in this linked security header group.

SG4 - M 99 - **UST**

A group of segments containing a link with security header segment group and the result of the security services applied to the message/package.

4. Segments Description

UST - M 1 - Security trailer

A segment establishing a link between security header and security trailer segment group, and stating the number of security segments in these groups.

UNT - M 1 - Message trailer

A service segment ending a message, giving the total number of segments and the control reference number of the message.

UNZ - M 1 - Interchange trailer

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

5. Segments Layout

This section describes each segment used in the EANCOM® AUTACK message. The original EDIFACT segment layout is listed. The appropriate comments relevant to the EANCOM® subset are indicated.

Notes:

1. The segments are presented in the sequence in which they appear in the message. The segment or segment group tag is followed by the (M)andatory / (C)onditional indicator, the maximum number of occurrences and the segment description.

2. Reading from left to right, in column one, the data element tags and descriptions are shown, followed by in the second column the EDIFACT status (M or C), the field format, and the picture of the data elements. These first pieces of information constitute the original EDIFACT segment layout.

   Following the EDIFACT information, EANCOM® specific information is provided in the third, fourth, and fifth columns. In the third column a status indicator for the use of (C)onditional EDIFACT data elements (see 2.1 through 2.3 below), in the fourth column the restricted indicator (see point 3 on the following page), and in the fifth column notes and code values used for specific data elements in the message.

2.1 (M)andatory data elements in EDIFACT segments retain their status in EANCOM®.

2.2 Additionally, there are five types of status for data elements with a (C)onditional EDIFACT status, whether for simple, component or composite data elements. These are listed below and can be identified when relevant by the following abbreviations:

- REQUIRED	**R**	Indicates that the entity is required and must be sent.
- ADVISED	**A**	Indicates that the entity is advised or recommended.
- DEPENDENT	**D**	Indicates that the entity must be sent in certain conditions, as defined by the relevant explanatory note.
- OPTIONAL	**O**	Indicates that the entity is optional and may be sent at the discretion of the user.
- NOT USED	**N**	Indicates that the entity is not used and should be omitted.

2.3 If a composite is flagged as **N, NOT USED**, all data elements within that composite will have blank status indicators assigned to them.

3. Status indicators detailed in the fourth column which directly relate to the code values detailed in the fifth **column** may have two values:

- RESTRICTED	*****	A data element marked with an asterisk (*) in the fourth column indicates that the listed codes in column five are the only codes available for use with this data element, in this segment, in this message.
- OPEN		All data elements where coded representation of data is possible and a restricted set of code values is not indicated are open (no asterisk in fourth column). The available codes are listed in the EANCOM® Data Elements and Code Sets Directory. Code values may be given as examples or there may be a note on the format or type of code to be used.

4. Different colours are used for the code values in the segment details: restricted codes are in red and open codes in blue.

5. Segments Layout

Segment number: 1

UNA - C 1 - Service string advice

Function:

The service string advice shall begin with the upper case characters UNA immediately followed by six characters in the order shown below. The space character shall not be used in positions 010, 020, 040, 050 or 060. The same character shall not be used in more than one position of the UNA.

		EDIFACT	GS1	*	Description
UNA1	Component data element separator	M an1	**M**	*	Used as a separator between component data elements contained within a composite data element (default value: ":")
UNA2	Data element separator	M an1	**M**	*	Used to separate two simple or composite data elements (default value: "+")
UNA3	Decimal mark	M an1	**M**	*	Used to indicate the character used for decimal notation (default value:".")
UNA4	Release character	M an1	**M**	*	Used to restore any service character to its original specification (value: "?").
UNA5	Repetition separator	M an1	**M**	*	Used to indicate the character used for repetition separation (value: " * ").
UNA6	Segment terminator	M an1	**M**	*	Used to indicate the end of segment data (default value: " ' ")

Segment Notes:

This segment is used to inform the receiver of the interchange that a set of service string characters which are different to the default characters are being used.
When using the default set of service characters, the UNA segment need not be sent. If it is sent, it must immediately precede the UNB segment and contain the four service string characters (positions UNA1, UNA2, UNA4 and UNA6) selected by the interchange sender.
Regardless of whether or not all of the service string characters are being changed every data element within this segment must be filled, (i.e., if some default values are being used with user defined ones, both the default and user defined values must be specified).
When expressing the service string characters in the UNA segment, it is not necessary to include any element separators.
The use of the UNA segment is required when using a character set other than level A.
UNA:+.?*'

5. Segments Layout

Segment number: 2

UNB - M 1 - Interchange header

Function:

To identify an interchange.

Notes:
1. S001/0002, shall be '4' to indicate this version of the syntax.
2. The combination of the values carried in data elements S002, S003 and 0020 shall be used to identify uniquely the interchange, for the purpose of acknowledgement.

		EDIFACT	GS1	*	Description
S001	SYNTAX IDENTIFIER	M	**M**		See Part I chapter 5.2.7 and segment notes.
0001	Syntax identifier	M a4	**M**	*	UNOA = UN/ECE level A UNOB = UN/ECE level B UNOC = UN/ECE level C UNOD = UN/ECE level D UNOE = UN/ECE level E UNOF = UN/ECE level F UNOG = UN/ECE level G UNOH = UN/ECE level H UNOI = UN/ECE level I UNOJ = UN/ECE level J UNOK = UN/ECE level K UNOW = UN/ECE level W UNOX = UN/ECE level X UNOY = UN/ECE level Y
0002	Syntax version number	M an1	**M**	*	4 = Version 4
0080	Service code list directory version number	C an..6	**N**		
0133	Character encoding, coded	C an..3	**N**		
S002	INTERCHANGE SENDER	M	**M**		
0004	Interchange sender identification	M an..35	**M**		GLN (n13)
0007	Identification code qualifier	C an..4	**R**	*	14 = GS1
0008	Interchange sender internal identification	C an..35	**O**		
0042	Interchange sender internal sub-identification	C an..35	**N**		
S003	INTERCHANGE RECIPIENT	M	**M**		
0010	Interchange recipient identification	M an..35	**M**		GLN (n13)
0007	Identification code qualifier	C an..4	**R**	*	14 = GS1
0014	Interchange recipient internal identification	C an..35	**O**		
0046	Interchange recipient internal sub-identification	C an..35	**N**		
S004	DATE AND TIME OF PREPARATION	M	**M**		
0017	Date	M n8	**M**		CCYYMMDD
0019	Time	M n4	**M**		HHMM
0020	Interchange control reference	M an..14	**M**		Unique reference identifying the interchange. Created

5. Segments Layout

Segment number: 2

		EDIFACT	GS1	*	Description
					by the interchange sender.
S005	RECIPIENT REFERENCE/ PASSWORD DETAILS	C	**O**		
0022	Recipient reference/password	M an..14	**M**		
0025	Recipient reference/password qualifier	C an2	**O**		
0026	Application reference	C an..14	**O**		Message identification if the interchange contains only one type of message.
0029	Processing priority code	C a1	**O**		A = Highest priority
0031	Acknowledgement request	C n1	**O**		1 = Requested
0032	Interchange agreement identifier	C an..35	**O**	*	EANCOM.....
0035	Test indicator	C n1	**O**		1 = Interchange is a test

Segment Notes:

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.
S001: The character encoding specified in basic code table of ISO/IEC 646 (7-bit coded character set for information interchange) shall be used for the interchange service string advice (if used) and up to and including the composite data element S001 'Syntax identifier' in the interchange header. The character repertoire used for the characters in an interchange shall be identified from the code value of data element 0001 in S001 'Syntax identifier' in the interchange header. The character repertoire identified does not apply to objects and/or encrypted data.
The default encoding technique for a particular repertoire shall be the encoding technique defined by its associated character set specification.
DE 0001: 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.
DE 0004, 0008, 0010 and 0014: Within EANCOM® the use of the Global Location Number (GLN) is recommended for the identification of the interchange sender and recipient.
DE 0008: 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.
DE 0014: The address for routing, provided beforehand by the interchange recipient, is used by the interchange sender to inform the recipient of the internal address, within the latter's systems, to which the interchange should be routed. It is recommended that the GLN be used for this purpose.
DE 0007: Identification (e.g. a division) specified by the recipient of the interchange, to be included if agreed, by the sender in response interchanges, to facilitate internal routing.
DE S004: The date and time specified in this composite should be the date and time at which the interchange sender prepared the interchange. This date and time may not necessarily be the same as the date and time of contained messages.
DE 0020: The interchange control reference number is generated by the interchange sender and is used to identify uniquely each interchange. Should the interchange sender wish to re-use interchange control reference numbers, it is recommended that each number be preserved for at least a period of three months before being re-used. In order to guarantee uniqueness, the interchange control reference number should always be linked to the interchange sender's identification (DE 0004).
DE S005: The use of passwords must first be agreed bilaterally by the parties exchanging the interchange.
DE 0026: 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 invoices). The reference used in this data element is assigned by the interchange sender.
DE 0031: 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

5. Segments Layout

Segment number: 2

due to syntax errors.
DE 0032: 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.

UNB+UNOC:4+5412345678908:14+8798765432106:14+20020102:1000+12345555+++++EANCOMREF 52'

5. Segments Layout

Segment number: 3

UNH - M 1 - Message header

Function:

To head, identify and specify a message.

Notes:
1. Data element S009/0057 is retained for upward compatibility. The use of S016 and/or S017 is encouraged in preference.
2. The combination of the values carried in data elements 0062 and S009 shall be used to identify uniquely the message within its group (if used) or if not used, within its interchange, for the purpose of acknowledgement.

		EDIFACT	GS1	*	Description
0062	Message reference number	M an..14	**M**		Sender's unique message reference. Sequence number of messages in the interchange. DE 0062 in UNT will have the same value. Generated by the sender.
S009	MESSAGE IDENTIFIER	M	**M**		
0065	Message type	M an..6	**M**	*	AUTACK = Secure authentication and acknowledgement message
0052	Message version number	M an..3	**M**	*	4 = Service message, version 4
0054	Message release number	M an..3	**M**	*	1 = First release
0051	Controlling agency, coded	M an..3	**M**	*	UN = UN/CEFACT
0057	Association assigned code	C an..6	**R**	*	EAN001 = GS1 version control number (GS1 Permanent Code)
0110	Code list directory version number	C an..6	**O**		This data element can be used to identify the codelist agreed by the interchange partners, e.g. EAN001 = EANCOM 2002 S4 codelist released on 01.12.2001 by GS1.
0113	Message type sub-function identification	C an..6	**N**		
0068	Common access reference	C an..35	**N**		
S010	STATUS OF THE TRANSFER	C	**N**		
0070	Sequence of transfers	M n..2			
0073	First and last transfer	C a1			
S016	MESSAGE SUBSET IDENTIFICATION	C	**N**		
0115	Message subset identification	M an..14			
0116	Message subset version number	C an..3			
0118	Message subset release number	C an..3			
0051	Controlling agency, coded	C an..3			
S017	MESSAGE IMPLEMENTATION GUIDELINE IDENTIFICATION	C	**N**		
0121	Message implementation guideline identification	M an..14			
0122	Message implementation guideline version number	C an..3			
0124	Message implementation	C an..3			

5. Segments Layout

Segment number: 3

		EDIFACT	GS1	*	Description
	guideline release number				
0051	Controlling agency, coded	C an..3			
S018	SCENARIO IDENTIFICATION	C	**N**		
0127	Scenario identification	M an..14			
0128	Scenario version number	C an..3			
0130	Scenario release number	C an..3			
0051	Controlling agency, coded	C an..3			

Segment Notes:

This segment is used to head, identify and specify a message.
DE's 0065, 0052, 0054, and 0051: Indicate that the message is an UNSM AUTACK under the control of the United Nations.

Example:
UNH+AUT00001+AUTACK:4:1:UN:EAN001'

5. Segments Layout

Segment number: 4

SG1	- M	99 -	USH-USA-SG2
USH	- M	1 -	Security header

Function:

To specify a security mechanism applied to a EDIFACT structure (i.e.: either message/package, group or interchange).

Notes:
1. 0541, if not present the default scope is the current security header segment group and the message body or object itself.
2. 0507, the original character set encoding of the EDIFACT structure when it was secured. If no value is specified, the character set encoding corresponds to that identified by the syntax identifier character repertoire in the UNB segment.
3. S500, two occurrences are possible: one for the security originator, one for the security recipient.
4. S500/0538, may be used to establish the key relationship between the sending and receiving parties.
5. S501, may be used as a security timestamp. It is security related and may differ from any dates and times that may appear elsewhere in the EDIFACT structure. It may be used to provide sequence integrity.

		EDIFACT	GS1	*	Description
0501	Security service, coded	M an..3	**M**	*	7 = Referenced EDIFACT structure non-repudiation of origin
0534	Security reference number	M an..14	**M**		Unique reference number assigned by the security originator to the security header group, security trailer group and the USY segment (USH, DE 0534; UST, DE 0534 and USY, DE 0534).
0541	Scope of security application, coded	C an..3	**R**	*	3 = Whole related message, package, group or interchange 6 = Part related message, package, group or interchange (GS1 Temporary Code) Specification of the scope of application of the security service defined in the security header.
0503	Response type, coded	C an..3	**N**		
0505	Filter function, coded	C an..3	**R**	*	2 = Hexadecimal filter Identification of the filtering function used to reversibly map any bit pattern to a restricted character set. The filter function describes how binary information (e.g., a digital signature) can be shown in a readable format. This is for example the case if the value "01111111 00111011" has no readable presentation and can be shown with the hexadecimal filter as "7F 3B".
0507	Original character set encoding, coded	C an..3	**R**	*	1 = ASCII 7 bit 2 = ASCII 8 bit 3 = Code page 850 (IBM PC Multinational) 4 = Code page 500 (EBCDIC Multinational No. 5) Identification of the character set in which the secured EDIFACT structure was encoded when security mechanisms were applied (i.e., when the digital signature was generated).
0509	Role of security provider, coded	C an..3	**N**		
S500	SECURITY IDENTIFICATION DETAILS	C	**N**		
0577	Security party qualifier	M an..3			

5. Segments Layout

Segment number: 4

		EDIFACT	GS1	*	Description
0538	Key name	C an..35			
0511	Security party identification	C an..512			
0513	Security party code list qualifier	C an..3			
0515	Security party code list responsible agency, coded	C an..3			
0586	Security party name	C an..35			
0586	Security party name	C an..35			
0586	Security party name	C an..35			
0520	Security sequence number	C an..35	**N**		
S501	SECURITY DATE AND TIME	C	**R**		
0517	Date and time qualifier	M an..3	**M**	*	1 = Security Timestamp Date and time when the signature was generated.
0338	Event date	C n..8	**R**		Date of event, format is CCYYMMDD.
0314	Event time	C an..15	**R**		Time of event, format is HHMMSS
0336	Time offset	C n4	**O**		UTC (Universal Co-ordinated Time) offset from event time. Format is HHMM. Shall be prefixed with '-' for negative offsets.

Segment Notes:

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

Example:
USH+7+1+3+1+2+1++++1:20011010:110522:0100'

5. Segments Layout

Segment number: 5

SG1	- M	99	- USH-USA-SG2
USA	- C	3	- Security algorithm

Function:

To identify a security algorithm, the technical usage made of it, and to contain the technical parameters required.

Notes:
1. S503, provides space for one parameter. The number of repetitions of S503 actually used will depend on the algorithm used. The order of the parameters is arbitrary but, in each case, the actual value is preceded by a coded algorithm parameter qualifier.

		EDIFACT	GS1	*	Description
S502	SECURITY ALGORITHM	M	**M**		
0523	Use of algorithm, coded	M an..3	**M**	*	1 = Owner hashing
0525	Cryptographic mode of operation, coded	C an..3	**R**	*	16 = DSMR Specification of the cryptographic mode of operation used for the algorithm. Note: The cryptographic mode of operation are the security functions authenticity, integrity and non-repudiation of origin. The digital signature includes all three security functions.
0533	Mode of operation code list identifier	C an..3	**R**	*	1 = UN/CEFACT
0527	Algorithm, coded	C an..3	**R**		6 = MD5 14 = RIPEMD-160 16 = SHA1 Identification of the algorithm in order to generate the hash value. The algorithms above are recommended.
0529	Algorithm code list identifier	C an..3	**R**	*	1 = UN/CEFACT
0591	Padding mechanism, coded	C an..3	**R**	*	7 = ISO 9796 #2 padding Note: "ISO 9796 #2 padding" specifies the technical standard which is facilitating the security service "digital signature scheme giving message recovery" specified in DE 0525.
0601	Padding mechanism code list identifier	C an..3	**R**	*	1 = UN/CEFACT
S503	ALGORITHM PARAMETER	C	**N**		
0531	Algorithm parameter qualifier	M an..3			
0554	Algorithm parameter value	M an..512			

Segment Notes:

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.

Example:
USA+1:16:1:6:1:7:1'

5. Segments Layout

Segment number: 6

SG1	- M	99	- USH-USA-SG2
SG2	- C	2	- USC-USA
USC	- M	1	- Certificate

Function:

To convey the public key and the credentials of its owner.

Dependency Notes:
1. D5(110,100) If first, then all

Notes:
2. 0536, if a full certificate (including the USR segment) is not used, the only data elements of the certificate shall be a unique certificate reference made of: the certificate reference (0536), the S500 identifying the issuer certification authority or the S500 identifying the certificate owner, including its public key name. In the case of a non-EDIFACT certificate data element 0545 shall also be present.
3. S500/0538, identifies a public key: either of the owner of this certificate, or the public key related to the private key used by the certificate issuer (certification authority or CA) to sign this certificate.
4. 0507, the original character set encoding of the certificate when it was signed. If no value is specified, the character set encoding corresponds to that identified by the character set repertoire standard.
5. 0543, the original character set repertoire of the certificate when it was signed. If no value is specified, the default is defined in the interchange header.
6. S505, when this certificate is transferred, it will use the default service characters defined in part 1 of ISO 9735, or those defined in the service string advice, if used. This data element may specify the service characters used when the certificate was signed. If this data element is not used then they are the default service characters.
7. S501, dates and times involved in the certification process. Four occurrences of this composite data element are possible: one for the certificate generation date and time, one for the certificate start of validity period, one for the certificate end of validity period, one for revocation date and time.

		EDIFACT	GS1	*	Description
0536	Certificate reference	C an..35	**O**		If an advanced electronic signature is used, the reference of the qualified certificate is given. This data element is used in combination with DE 0577 (code value 4 = Authenticating party).
S500	SECURITY IDENTIFICATION DETAILS	C	**R**		
0577	Security party qualifier	M an..3	**M**	*	3 = Certificate owner 4 = Authenticating party Identification of the role of the security parties (signature key owner or trusted third party).
0538	Key name	C an..35	**O**		Identification of the public key to verify the digital signature by the recipient.
0511	Security party identification	C an..512	**O**		Identification of the trusted third party (trust center) issuing the certificate identified in DE 0536. For identification of parties it is recommended to use GLN - Format n13.
0513	Security party code list qualifier	C an..3	**D**	*	2 = GS1 ZZZ = Mutually agreed
0515	Security party code list responsible agency, coded	C an..3	**N**		
0586	Security party name	C an..35	**N**		
0586	Security party name	C an..35	**N**		
0586	Security party name	C an..35	**N**		
0545	Certificate syntax and version, coded	C an..3	**D**		3 = X.509 Where it is decided to refer to a non-EDIFACT

5. Segments Layout

Segment number: 6

		EDIFACT	GS1	*	Description
					certificate (such as X.509), the certificate syntax and version shall be identified in data element 0545 of the USC segment. Such certificates may be conveyed in an EDIFACT package.
0505	Filter function, coded	C an..3	**N**		
0507	Original character set encoding, coded	C an..3	**N**		
0543	Certificate original character set repertoire, coded	C an..3	**N**		
0546	User authorisation level	C an..35	**N**		
S505	SERVICE CHARACTER FOR SIGNATURE	C	**N**		
0551	Service character for signature qualifier	M an..3			
0548	Service character for signature	M an..4			
S501	SECURITY DATE AND TIME	C	**N**		
0517	Date and time qualifier	M an..3			
0338	Event date	C n..8			
0314	Event time	C an..15			
0336	Time offset	C n4			
0567	Security status, coded	C an..3	**N**		
0569	Revocation reason, coded	C an..3	**N**		

Segment Notes:

This segment either contains information regarding the certificate, and identifies the certification authority which has generated the certificate, or is used to identify bilaterally interchanged signature keys.

1. Use of USC for certificate reference:
A certificate reference (DE 0536) and trusted third party (DEG S500, DE 0577 = 4 and DEG S500, DE 511) can be identified.
Example 1:
USC+AXZ4711+4::5412345000006:2+3'

2. Use of USC for reference to signature keys:
Identification of the name of the signature key in DEG S500, DE 0538 (DEG S500, DE 0577 = 3).
The interchange of signature keys and the references have to be bilaterally agreed between the partners.
Example 2:
USC++3:PUBLIC KEY 01'

5. Segments Layout

Segment number: 7

SG1	- M	99 -	USH-USA-SG2
SG2	- C	2 -	USC-USA
USA	- C	3 -	Security algorithm

Function:

To identify a security algorithm, the technical usage made of it, and to contain the technical parameters required.

Notes:
1. S503, provides space for one parameter. The number of repetitions of S503 actually used will depend on the algorithm used. The order of the parameters is arbitrary but, in each case, the actual value is preceded by a coded algorithm parameter qualifier.

		EDIFACT	GS1	*	Description
S502	SECURITY ALGORITHM	M	**M**		
0523	Use of algorithm, coded	M an..3	**M**	*	6 = Owner signing
0525	Cryptographic mode of operation, coded	C an..3	**R**	*	16 = DSMR Specification of the cryptographic mode of operation used for the algorithm. Note: The cryptographic mode of operation are the security functions authenticity, integrity and non-repudiation of origin. The digital signature includes all three security functions.
0533	Mode of operation code list identifier	C an..3	**R**	*	1 = UN/CEFACT
0527	Algorithm, coded	C an..3	**R**		10 = RSA 17 = ECC Identification of the algorithm in order to generate the digital signature. The algorithms above are recommended.
0529	Algorithm code list identifier	C an..3	**R**	*	1 = UN/CEFACT
0591	Padding mechanism, coded	C an..3	**R**	*	7 = ISO 9796 #2 padding Note: "ISO 9796 #2 padding" specifies the technical standard which is facilitating the security service "digital signature scheme giving message recovery" specified in DE 0525.
0601	Padding mechanism code list identifier	C an..3	**R**	*	1 = UN/CEFACT
S503	ALGORITHM PARAMETER	C	**N**		
0531	Algorithm parameter qualifier	M an..3			
0554	Algorithm parameter value	M an..512			

Segment Notes:

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 digital signature.
At least one occurrence of this segment is mandatory.

Example:
USA+6:16:1:10:1:7:1'

5. Segments Layout

Segment number: 8

USB - M 1 - Secured data identification					
Function: To contain details related to the AUTACK.					
		EDIFACT	GS1	*	Description
0503	Response type, coded	M an..3	**M**	*	1 = No acknowledgement required
S501	SECURITY DATE AND TIME	C	**N**		
0517	Date and time qualifier	M an..3			
0338	Event date	C n..8			
0314	Event time	C an..15			
0336	Time offset	C n4			
S002	INTERCHANGE SENDER	M	**M**		
0004	Interchange sender identification	M an..35	**M**		For identification of parties it is recommended to use GLN - Format n13.
0007	Identification code qualifier	C an..4	**R**	*	14 = GS1
0008	Interchange sender internal identification	C an..35	**N**		
0042	Interchange sender internal sub-identification	C an..35	**N**		
S003	INTERCHANGE RECIPIENT	M	**M**		
0010	Interchange recipient identification	M an..35	**M**		For identification of parties it is recommended to use GLN - Format n13.
0007	Identification code qualifier	C an..4	**R**	*	14 = GS1
0014	Interchange recipient internal identification	C an..35	**N**		
0046	Interchange recipient internal sub-identification	C an..35	**N**		
Segment Notes: This segment shall contain identification of the interchange sender and interchange recipient. The interchange sender and interchange recipient in USB shall refer to the sender and the recipient of the interchange in which the AUTACK is present, in order to secure this information. Example: USB+1++5412345123450:14+5411234512300:14'					

5. Segments Layout

Segment number: 9

SG3	- M	9999 -	USX-USY
USX	- M	1 -	Security references

Function:

To refer to the secured EDIFACT structure and its associated date and time.

Dependency Notes:
1. D5(050,040) If first, then all
2. D1(070,090) One and only one
3. D5(060,040) If first, then all
4. D5(080,070) If first, then all

		EDIFACT	GS1	*	Description
0020	Interchange control reference	M an..14	**M**		Unique reference number of interchange containing the data to which the security service was applied (UNB, DE 0020).
S002	INTERCHANGE SENDER	C	**R**		
0004	Interchange sender identification	M an..35	**M**		Identification of the party sending the interchange which contains the data to which security services were applied. It is recommended to use GLN - Format n13.
0007	Identification code qualifier	C an..4	**R**	*	14 = GS1
0008	Interchange sender internal identification	C an..35	**N**		
0042	Interchange sender internal sub-identification	C an..35	**N**		
S003	INTERCHANGE RECIPIENT	C	**R**		
0010	Interchange recipient identification	M an..35	**M**		Identification of the party receiving the interchange which contains the data to which security services were applied. It is recommended to use GLN - Format n13.
0007	Identification code qualifier	C an..4	**R**	*	14 = GS1
0014	Interchange recipient internal identification	C an..35	**N**		
0046	Interchange recipient internal sub-identification	C an..35	**N**		
0048	Group reference number	C an..14	**D**		Reference to a message group (UNG to UNE) containing data to which the security service was applied (UNG, DE 0048).
S006	APPLICATION SENDER IDENTIFICATION	C	**N**		
0040	Application sender identification	M an..35			
0007	Identification code qualifier	C an..4			
S007	APPLICATION RECIPIENT IDENTIFICATION	C	**N**		
0044	Application recipient identification	M an..35			
0007	Identification code qualifier	C an..4			
0062	Message reference number	C an..14	**D**		Reference number of a message (UNH to UNT) to which the security service was applied (UNH, DE

5. Segments Layout

Segment number: 9

		EDIFACT	GS1	*	Description
					0062 of this message).
S009	MESSAGE IDENTIFIER	C	**N**		
0065	Message type	M an..6			
0052	Message version number	M an..3			
0054	Message release number	M an..3			
0051	Controlling agency, coded	M an..3			
0057	Association assigned code	C an..6			
0110	Code list directory version number	C an..6			
0113	Message type sub-function identification	C an..6			
0800	Package reference number	C an..35	**N**		
S501	SECURITY DATE AND TIME	C	**N**		
0517	Date and time qualifier	M an..3			
0338	Event date	C n..8			
0314	Event time	C an..15			
0336	Time offset	C n4			

Segment Notes:

This segment shall contain references to EDIFACT structures (i.e., interchanges, groups or messages) to which security services were applied.

The USX segment of the AUTACK message refers to a whole interchange, a message group within this interchange or a message in the interchange. Any reference made has to be non-ambiguous; if necessary the reference on a higher hierarchical level has to be indicated.

The USX segment enables the use following references:
· DE 0020 Interchange reference number
· DE 0048 Group reference number
· DE 0062 Message reference number

Application of the interchange reference number of the UNB segment:

Definition: Unique reference number generated by the sender in order to identify the interchange to which security services were applied or which contains messages or groups to which security services were applied.

The message recipient can combine the interchange reference number (DE 0020) and the sender identification (DE 0004) in order to ensure unambiguousness of the reference.

The interchange reference number as the only reference number is used if the security function (i.e., the digital signature) applies to the whole interchange. If the reference data and the AUTACK message are sent in different interchanges, then the interchange reference number is also mandatory, if the security function applies to groups or messages. If the reference data (messages or groups) and the AUTACK message are sent in the same interchange, the interchange reference number is not necessary.

Application of the group reference number of the UNG segment:

Definition: Unique reference number of a group of messages within an interchange to which security services were applied.
In this case to the USX segment refers to the unambiguous group reference number of the sender within an interchange. The group reference number is used if the security function (i.e., the digital signature) was applied to a group of messages.

5. Segments Layout

Segment number: 9

Application of the message reference number of the UNH segment:

Definition: Unique reference number of a message within an interchange to which the security service was applied, generated by the sender.
In this case to the USX segment refers to the unambiguous message reference number of the sender within an interchange.
If the security service applies to every single message,
1) a separate AUTACK message needs to be sent for every message
or
2) the segment group 3 (USX/USY) has to be repeated for every message

A separate AUTACK message for every message is necessary, if the messages on their way to the recipient are forwarded within another interchange (e.g., distribution by a clearing centre).

Example:
USX+DAT001+5412345123450:14+5411234512300:14+GRP002+++MES003'

5. Segments Layout

Segment number: 10

SG3	- M	9999 -	USX-USY
USY	- M	9 -	Security on references

Function:

To identify the applicable header, and to contain the security result and/or to indicate the possible cause of security rejection for the referred value.

Dependency Notes:
1. D3(020,030) One or more

		EDIFACT	GS1	*	Description
0534	Security reference number	M an..14	**M**		Unique reference number assigned by the security originator to a pair of security header (USH, DE 0534) and security trailer groups (UST, DE 0534) as well as the value in this DE.
S508	VALIDATION RESULT	C	**R**		
0563	Validation value, qualifier	M an..3	**M**	*	1 = Unique validation value
0560	Validation value	C an..512	**R**		Security result corresponding to the security service specified, i.e., the value generated from the hash value of the data referenced in the USX segment with the private key of the signature originator specified in the USC segment. If necessary, this value shall be filtered by an appropriate filter function.
0571	Security error, coded	C an..3	**N**		

Segment Notes:

This segment contains a link to the security header group and the result of the security services applied to the referenced EDIFACT structure (i.e., the digital signature) as specified in this linked security header group.

Example:
USY+1+1:139B7CB7...C72B03CE5F'

5. Segments Layout

Segment number: 11

SG4	- M	99	- UST
UST	- M	1	- Security trailer

Function:

To establish a link between security header and security trailer segment groups.

Notes:
1. 0534, the value shall be identical to the value in 0534 in the corresponding USH segment.

		EDIFACT	GS1	*	Description
0534	Security reference number	M an..14	**M**		Unique reference number assigned by the security originator to the security header group, security trailer group and the USY segment (USH, DE 0534; UST, DE 0534 and USY, DE 0534).
0588	Number of security segments	M n..10	**M**		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.

Segment Notes:

A segment establishing a link between security header and security trailer segment group, and stating the number of security segments in these groups.

Example:
UST+1+5'

5. Segments Layout

Segment number: 12

UNT - M 1 - Message trailer

Function:

To end and check the completeness of a message.

Notes:
1. 0062, the value shall be identical to the value in 0062 in the corresponding UNH segment.

		EDIFACT	GS1	*	Description
0074	Number of segments in a message	M n..10	**M**		The total number of segments in the message is detailed here.
0062	Message reference number	M an..14	**M**		The message reference number detailed here should equal the one specified in the UNH segment.

Segment Notes:

A service segment ending a message, giving the total number of segments and the control reference number of the message.

Example:
UNT+10+AUT00001'

5. Segments Layout

Segment number: 13

UNZ - M 1 - Interchange trailer

Function:

To end and check the completeness of an interchange.

Notes:
1. 0020, the value shall be identical to the value in 0020 in the corresponding UNB segment.

		EDIFACT	GS1	*	Description
0036	Interchange control count	M n..6	**M**		Number of messages or functional groups within an interchange.
0020	Interchange control reference	M an..14	**M**		Identical to DE 0020 in UNB segment.

Segment Notes:

This segment is used to provide the trailer of an interchange.
DE 0036: If functional groups are used, this is the number of functional groups within the interchange. If functional groups are not used, this is the number of messages within the interchange.
UNZ+5+12345555'

6. Examples

The following examples will show how the message type AUTACK can be used in order to transport the digital signature and the information necessary for signature verification by the recipient. There are various scenarios and possibilities how to use the AUTACK in relation to the data to which security services were applied. The appropriate scenario depends on the technical and legal requirements.

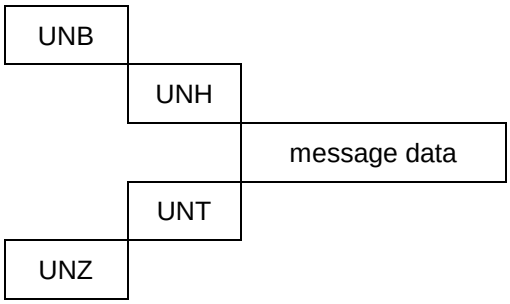
Example 1

Two interchanges are transmitted. The first interchange contains the data secured, the second interchange contains the AUTACK message.

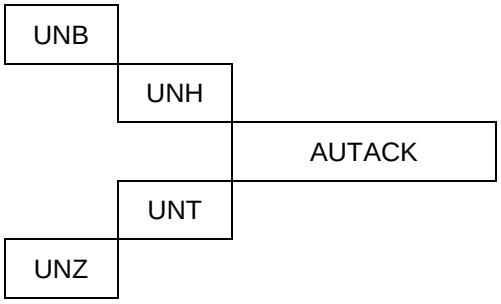
This example is recommended if

- the data secured and the AUTACK do not use the same EDIFACT syntax version;
- for technical or organisational reasons the data secured and the AUTACK are generated separately;
- for legal reasons the data secured and the AUTACK must be generated and sent separately.

Structure:



Interchange containing the data secured



Interchange containing the AUTACK message

6. Examples

EANCOM® realisation:

message data:

UNA:+.? '	Service string advice, syntax 3
UNB+UNOA:3+5412345678908:14+8798765432106:14+20020102:1000+INT12345'	Interchange header of the syntax 3 interchange INT12345.
UNH+ME0001+INVOIC:D:96A:UN:EAN008'	Message header of an INVOIC message, the message number is ME0001
....	
UNT+7+ME0001'	Message trailer
UNZ+1+12345'	Interchange trailer

security data:

UNA:+.?*'	Service string advice, syntax 4
UNB+UNOA:4+5412345678908:14+8798765432106:14+20020102:1015+INT12346’	Interchange header of the syntax 4 interchange INT12346.
UNH+AUT0001+AUTACK:4:1:UN:EAN001'	Message header of the service message AUTACK
USH+7+1+3+1+2+1++++1:20020102:100522:0100'	Security header, • security service ”non-repudiation of origin to a referenced EDIFACT structure” is applied, • the security function applies to the whole referenced message or interchange, • for filtering the signature a hexadecimal filter is used, • the original character set encoding of the EDIFACT structure was ASCII 7 bit • security time stamp is 2nd January 2002, 10:05:22
USA+1:16:1:6:1:7:1'	The hash algorithm applied to the EDIFACT structure by the sender is SHA 1, the padding mechanism is specified in ISO 9796 # 2.
USC+AXZ4711+4::5412345000006:2+3’	The reference of the certificate issued by the trust centre identified with the GLN 5412345000006 is AXZ4711. The syntax of the certificate is X.509.
USA+6:16:1:10:1:7:1'	The algorithm used for generating the signature is RSA, the padding mechanism is specified in ISO 9796 # 2.

6. Examples

USB+1++5412345678908:14+8798765432106:14	The sender and recipient of the interchange in which the AUTACK is present are identified with the GLNs 5412345678908 and 8798765432106.
USX+INT12345+5412345678908:14+8798765432106:14++++ ME0001'	The referenced message ME 0001 to which security functions were applied is within interchange INT12345. The sender and recipient of the interchange in which the referenced message is present are identified with the GLNs 5412345678908 and 8798765432106.
USY+1+1:139B7CB.....7C72B03CE5F'	The digital signature is 139B7CB.....7C72B03CE5F.
UST+1+5'	The number of security segments in the segment groups 1, 2 and 4 equals 5.
UNT+10+ AUT0001'	Message trailer, the total number of segments equals 10.
UNZ+1+INT12346’	Interchange trailer

6. Examples

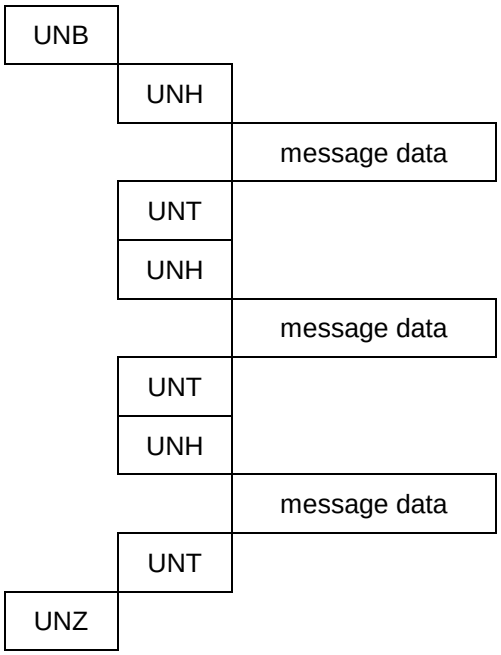
Example 2

Two interchanges are transmitted. The first interchange contains three messages to be secured, the second interchange contains the AUTACK message.

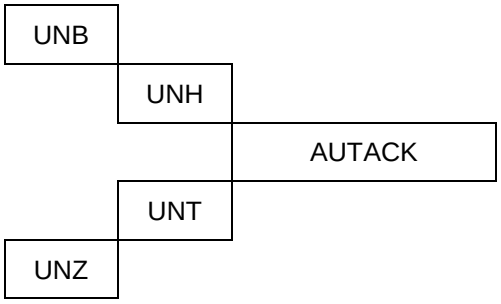
This example is recommended if

- the data secured and the AUTACK do not use the same EDIFACT syntax version;
- for technical or organisational reasons the data secured and the AUTACK are generated separately;
- for legal reasons the data secured and the AUTACK must be generated and sent separately;
- several messages in one interchange should be signed at once.

Structure:



Interchange containing the data secured



Interchange containing the AUTACK message

6. Examples

EANCOM® realisation:

message data:

UNA:+.? '	Service string advice, syntax 3
UNB+UNOA:3+5412345678908:14+8798765432106:14+20020102:1000+12345'	Interchange header of the syntax 3 interchange INT12345.
UNH+ME0001+INVOIC:D:96A:UN:EAN008'	Message header of the first INVOIC message, the message number is ME0001.
....	
UNT+7+ME0001'	Message trailer of the first message
UNH+ME0002+INVOIC:D:96A:UN:EAN008'	Message header of the second INVOIC message, the message number is ME0002.
....	
UNT+7+ME0002'	Message trailer of the second message
UNH+ME0003+INVOIC:D:96A:UN:EAN008'	Message header of the third INVOIC message, the message number is ME0003.
....	
UNT+7+ME0003'	Message trailer of the third message
UNZ+3+12345'	Interchange trailer

security data:

UNA:+.?*'	Service string advice, syntax 4
UNB+UNOA:4+5412345678908:14+8798765432106:14+20020102:1002+12346’	Interchange header of the syntax 4 interchange INT12346.
UNH+AUT0001+AUTACK:4:1:UN:EAN001'	Message header of the service message AUTACK
USH+7+1+3+1+2+1++++1:20020102:100522:0100'	Security header, • security service ”non-repudiation of origin to a referenced EDIFACT structure” is applied, • the security function applies to the whole referenced message or interchange, • for filtering the signature a hexadecimal filter is used, • the original character set encoding of the EDIFACT structure was ASCII 7 bit • security time stamp is 2nd January 2002, 10:05:22

6. Examples

USA+1:16:1:6:1:7:1'	The hash algorithm applied to the EDIFACT structure by the sender is SHA 1, the padding mechanism is specified in ISO 9796 # 2.
USC+AXZ4711+4::541234500006:2+3'	The reference to the certificate issued by the trust centre identified with the GLN 5412345000006 is AXZ4711. The syntax of the certificate is X.509.
USA+6:16:1:10:1:7:1'	The algorithm used for generating the signature is RSA, the padding mechanism is specified in ISO 9796 # 2.
USB+1++5412345678908:14+8798765432106:14'	The sender and recipient of the interchange in which the AUTACK is present are identified with the GLNs 5412345678908 and 8798765432106.
USX+INT12435+5412345678908:14+8798765432106:14'	The referenced messages to which security functions were applied are within interchange INT12345. The sender and recipient of the referenced interchange are identified with the GLNs 5412345678908 and 8798765432106.
USY+1+1:139B7CB.....7C72B03CE5F'	The digital signature is 139B7CB.....7C72B03CE5F.
UST+1+5'	The number of security segments in the segment groups 1, 2 and 4 equals 5.
UNT+10+AUT0001'	Message trailer, the total number of segments equals 10.
UNZ+1+12346'	Interchange trailer

6. Examples

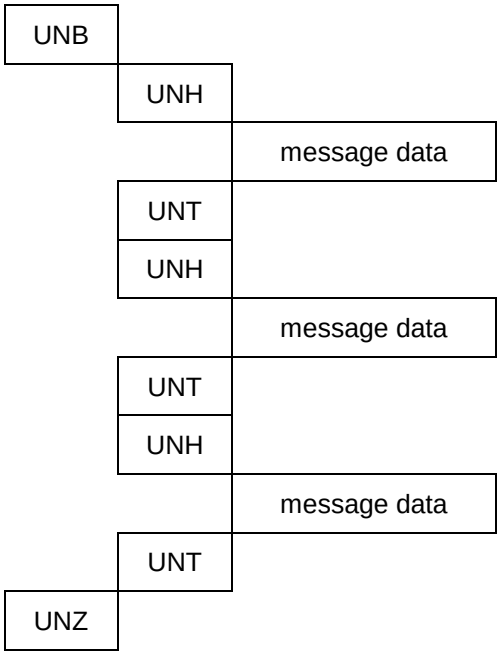
Example 3

Two interchanges are transmitted. The first interchange contains three messages to be secured, the second interchange contains the AUTACK message. In order to transmit the digital signature for every single message, segment group 3 of the AUTACK message is repeated three times.

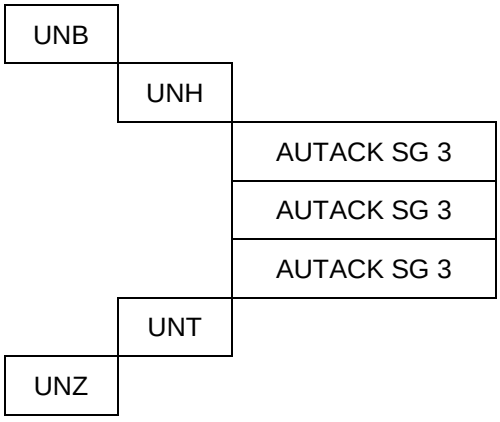
This example is recommended if

- the data secured and the AUTACK do not use the same EDIFACT syntax version;
- for technical or organisational reasons the data secured and the AUTACK are generated separately;
- for legal reasons the data secured and the AUTACK must be generated and sent separately;
- every single message in one interchange should be signed separately (e.g., for legal reasons).

Structure:



Interchange containing the data secured



Interchange containing the AUTACK message

6. Examples

EANCOM® realisation:

message data:

UNA:+.? '	Service string advice, syntax 3
UNB+UNOA:3+5412345678908:14+8798765432106:14+20020102:1000+12345'	Interchange header of the syntax 3 interchange INT12345.
UNH+ME0001+INVOIC:D:96A:UN:EAN008'	Message header of the first INVOIC message, the message number is ME0001.
....	
UNT+7+ME0001'	Message trailer of the first message
UNH+ME0002+INVOIC:D:96A:UN EAN008'	Message header of the second INVOIC message, the message number is ME0002.
....	
UNT+7+ME0002'	Message trailer of the second message
UNH+ME0003+INVOIC:D:96A:UN EAN008'	Message header of the third INVOIC message, the message number is ME0003.
....	
UNT+7+ME0003'	Message trailer of the third message
UNZ+3+12345'	Interchange trailer

security data:

UNA:+.?*'	Service string advice, syntax 4
UNB+UNOC:4+5412345678908:14+8798765432106:14+20020102:1002+12346’	Interchange header of the syntax 4 interchange INT12346.
UNH+AUT0001+AUTACK:4:1:UN:EAN001'	Message header of the service message AUTACK
USH+7+1+3+1+2+1++++1:20020102:100522:0100'	Security header, • security service ”non-repudiation of origin to a referenced EDIFACT structure” is applied, • the security function applies to the whole referenced message or interchange, • for filtering the signature a hexadecimal filter is used, • the original character set encoding of the EDIFACT structure was ASCII 7 bit • security time stamp is 2nd January 2002, 10:05:22

6. Examples

USA+1:16:1:6:1:7:1'	The hash algorithm applied to the EDIFACT structure by the sender is SHA 1, the padding mechanism is specified in ISO 9796 # 2.
USC+AXZ4711+4::541234500006:2+3'	The reference to the certificate issued by the trust centre identified with the GLN 5412345000006 is AXZ4711. The syntax of the certificate is X.509.
USA+6:16:1:10:1:7:1'	The algorithm used for generating the signature is RSA, the padding mechanism is specified in ISO 9796 # 2.
USB+1++5412345678908:14+8798765432106:14'	The sender and recipient of the interchange in which the AUTACK is present are identified with the GLNs 5412345678908 and 8798765432106.
USX+INT12435+5412345678908:14+8798765432106:14++++ME0001'	The first referenced message ME0001 to which security functions were applied is within interchange INT12345. The sender and recipient of the interchange in which the referenced message is present are identified with the GLNs 5412345678908 and 8798765432106.
USY+1+1:139B7CB7.....C72B03CE5F'	The digital signature of the first message is 139B7CB.....7C72B03CE5F.
USX+INT12435+5412345678908:14+8798765432106:14++++ME0002'	The second referenced message ME0002 to which security functions were applied is within interchange INT12345. The sender and recipient of the interchange in which the referenced message is present are identified with the GLNs 5412345678908 and 8798765432106.
USY+1+1:145D8BB.....2B69B38DC6A'	The digital signature of the second message is 145D8BB.....2B69B38DC6A.
USX+INT12435+5412345678908:14+8798765432106:14++++ME0003'	The third referenced message ME0003 to which security functions were applied is within interchange INT12345. The sender and recipient of the interchange in which the referenced message is present are identified with the GLNs 5412345678908 and 8798765432106.
USY+1+1:186A3DC.....4C54B59CE4E'	The digital signature of the third message is 186A3DC.....4C54B59CE4E.
UST+1+5'	The number of security segments in the segment groups 1, 2 and 4 equals 5.
UNT+14+AUT0001'	Message trailer, the total number of segments equals 14.
UNZ+1+123456'	Interchange trailer

6. Examples

Example 4

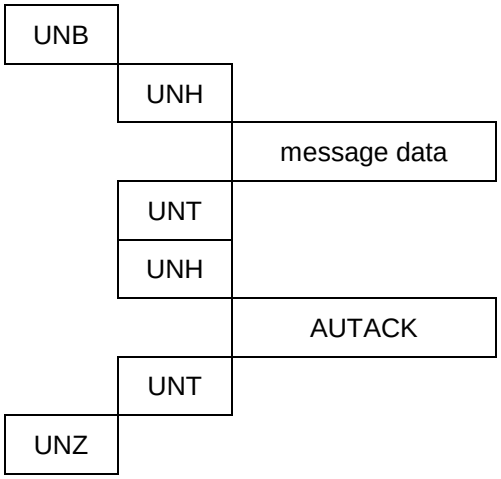
Message data and AUTACK are transmitted in one interchange. The interchange contains one AUTACK message and one message to be secured.

This example is recommended if

- the data secured and the AUTACK both use EDIFACT syntax version 4;
- for technical or organisational reasons the data secured and the AUTACK must be sent together;
- for legal reasons the data secured and the AUTACK must be generated and sent in one interchange.

The advantage of this scenario is that the signature can be verified directly, because the message and the signature information do not need to be matched by the recipient.

Structure:



EANCOM® realisation:

UNA:+.?*'	Service string advice, syntax 4
UNB+UNOC:4+5412345678908:14+87987654321 06:14+20020102:1015+12346’	Interchange header of the syntax 4 interchange INT12346.
UNH+ME0001+INVOIC:D:01B:UN:EAN010'	Message header of the an INVOIC message, the message number is ME0001.
....	
UNT+7+ME0001'	Message trailer of the INVOIC message
UNH+AUT0001+AUTACK:4:1:UN.EAN001'	Message header of the service message AUTACK

6. Examples

USH+7+1+3+1+2+1++++1:20020102:100522:0100'	Security header, • security service ”non-repudiation of origin to a referenced EDIFACT structure” is applied, • the security function applies to the whole referenced message or interchange, • for filtering the signature a hexadecimal filter is used, • the original character set encoding of the EDIFACT structure was ASCII 7 bit • security time stamp is 2nd January 2002, 10:05:22
USA+1:16:1:6:1:7:1'	The hash algorithm applied to the EDIFACT structure by the sender is SHA 1, the padding mechanism is specified in ISO 9796 # 2.
USC+AXZ4711+4::541234500006:2+3'	The reference to the certificate issued by the trust centre identified with the GLN 5412345000006 is AXZ4711. The syntax of the certificate is X.509.
USA+6:16:1:10:1:7:1'	The algorithm used for generating the signature is RSA, the padding mechanism is specified in ISO 9796 # 2.
USB+1++5412345678908:14+8798765432106:14'	The sender and recipient of the interchange in which the AUTACK is present are identified with the GLNs 5412345678908 and 8798765432106.
USX+INT12436+5412345678908:14+8798765432106:14++++ME0001'	The referenced message ME0001 to which security functions were applied is within interchange INT12345. The sender and recipient of the interchange in which the referenced message is present are identified with the GLNs 5412345678908 and 8798765432106.
USY+1+1:139B7CB.....7C72B03CE5F'	The digital signature is 139B7CB.....7C72B03CE5F.
UST+1+5'	The number of security segments in the segment groups 1, 2 and 4 equals 5.
UNT+10+AUT0001'	Message trailer, the total number of segments equals 10.
UNZ+2+12346'	Interchange trailer

6. Examples

Example 5

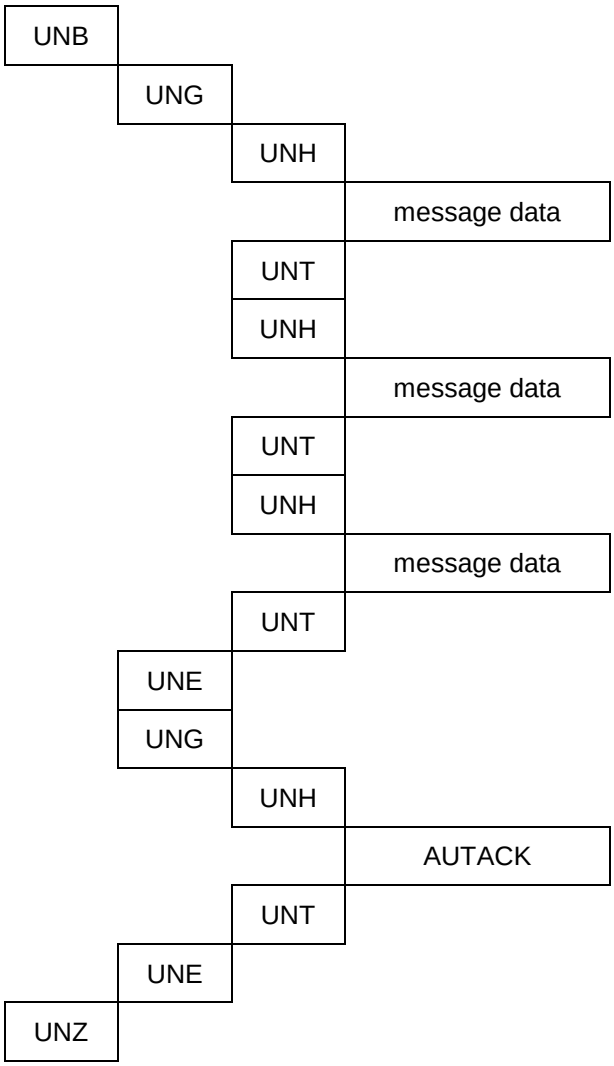
Message data and AUTACK are transmitted in one interchange. The interchange contains two groups of messages. The first group contains the data to be secured, the second group contains the AUTACK message. The security function applies to the group of messages.

This example is recommended if

- the data secured and the AUTACK both use EDIFACT syntax version 4;
- for technical or organisational reasons the data secured and the AUTACK must be sent together;
- for legal reasons the data secured and the AUTACK must be generated and sent in one interchange;
- several messages in one interchange should be signed at once.

The advantage of this scenario is, that the signature can be verified directly, because the message and the signature information do not need to be matched by the recipient.

Structure:



6. Examples

EANCOM® realisation:

UNA:+.?*'	Service string advice, syntax 4
UNB+UNOC:4+5412345678908:14+8798765432106:14+20020102:1015+12346'	Interchange header of the syntax 4 interchange INT12346.
UNG+INVOIC+5412345678908:14+8798765432106:14+20020102:1015+GRP0001+UN+D:01B:EAN010'	Message group header of the message group GRP0001, containing INVOIC messages
UNH+ME0001+INVOIC:D:01B:UN:EAN010'	Message header of the first INVOIC message, the message number is ME0001.
....	
UNT+7+ME0001'	Message trailer of the first message
UNH+ME0002+INVOIC:D:01B:UN:EAN010'	Message header of the second INVOIC message, the message number is ME0002.
....	
UNT+7+ME0002'	Message trailer of the second message
UNH+ME0003+INVOIC:D:01B:UN:EAN010'	Message header of the third INVOIC message, the message number is ME0003.
....	
UNT+7+ME0003'	Message trailer of the third message
UNE+3+GRP0001'	Message group trailer of the first group
UNG+AUTACK+5412345678908:14+8798765432106:14+20020102:1015+GRP0002+UN+4:1:EAN001'	Message group header of the message group GRP0002, containing the AUTACK message
UNH+AUT0001+AUTACK:4:1:UN:EAN001'	Message header of the service message AUTACK
USH+7+1+3+1+2+1++++1:20020102:100522:0100'	Security header, • security service ”non-repudiation of origin to a referenced EDIFACT structure” is applied, • the security function applies to the whole referenced message or interchange, • for filtering the signature a hexadecimal filter is used, • the original character set encoding of the EDIFACT structure was ASCII 7 bit • security time stamp is 2nd January 2002, 10:05:22
USA+1:16:1:6:1:7:1'	The hash algorithm applied to the EDIFACT structure by the sender is SHA 1, the padding mechanism is specified in ISO 9796 # 2.

6. Examples

USC+AXZ4711+4::541234500006:2+3'	The reference to the certificate issued by the trust centre identified with the GLN 5412345000006 is AXZ4711. The syntax of the certificate is X.509.
USA+6:16:1:10:1:7:1'	The algorithm used for generating the signature is RSA, the padding mechanism is specified in ISO 9796 # 2.
USB+1++5412345678908:14+8798765432106:14'	The sender and recipient of the interchange in which the AUTACK is present are identified with the GLNs 5412345678908 and 8798765432106.
USX+INT12436+5412345678908:14+879876543210 6:14+GRP0001'	The referenced group of messages GRP0001 to which security functions were applied is within interchange INT12346. The sender and recipient of the interchange in which the referenced group is present are identified with the GLNs 5412345678908 and 8798765432106.
USY+1+1:139B7CB7.....C72B03CE5F'	The digital signature of the group of messages is 139B7CB.....7C72B03CE5F.
UST+1+5'	The number of security segments in the segment groups 1, 2 and 4 equals 5.
UNT+10+AUT0001'	Message trailer, the total number of segments equals 10.
UNE+1+GRP0002'	Message group trailer of the second group
UNZ+4+12346'	Interchange trailer

6. Examples

Example 6

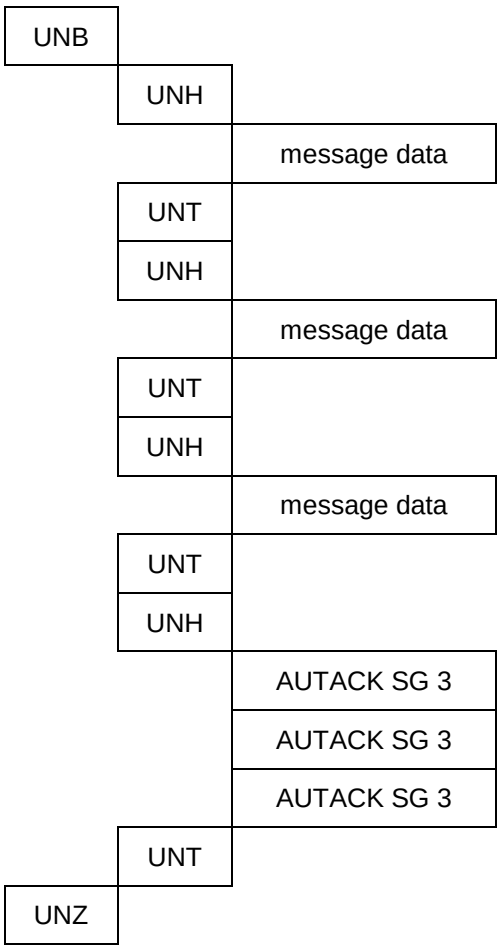
Message data and AUTACK are transmitted in one interchange. The interchange contains one AUTACK message and three messages to be secured. Within the AUTACK (repetition of SG 3) the signature information on every single message is transmitted.

This example is recommended if

- the data secured and the AUTACK both use EDIFACT syntax version 4;
- for technical or organisational reasons the data secured and the AUTACK must be sent together;
- for legal reasons the data secured and the AUTACK must be generated and sent in one interchange;
- every single message in one interchange should to be signed separately (e.g. for legal reasons).

The advantage of this scenario is that the signature can be verified directly and the message and the signature information do not need to be matched by the recipient.

Structure:



6. Examples

EANCOM® realisation:

UNA:+.?*'	Service string advice, syntax 4
UNB+UNOC:4+5412345678908:14+87987654321 06:14+20020102:1015+12346'	Interchange header of the syntax 4 interchange INT12346.
UNH+ME0001+INVOIC:D:01B:UN:EAN010'	Message header of the first INVOIC message, the message number is ME0001.
....	
UNT+7+ME0001'	Message trailer of the first message
UNH+ME0002+INVOIC:D:01B:UN:EAN010'	Message header of the second INVOIC message, the message number is ME0002.
....	
UNT+7+ME0002'	Message trailer of the second message
UNH+ME0003+INVOIC:D:01B:UN:EAN010'	Message header of the third INVOIC message, the message number is ME0003.
....	
UNT+7+ME0003'	Message trailer of the third message
UNH+AUT0001+AUTACK:4:1:UN:EAN001'	Message header of the service message AUTACK
USH+7+1+3+1+2+1++++1:20020102:100522:0100'	Security header, • security service "non-repudiation of origin to a referenced EDIFACT structure" is applied, • the security function applies to the whole referenced message or interchange, • for filtering the signature a hexadecimal filter is used, • the original character set encoding of the EDIFACT structure was ASCII 7 bit • security time stamp is 2nd January 2002, 10:05:22
USA+1:16:1:6:1:7:1'	The hash algorithm applied to the EDIFACT structure by the sender is SHA 1, the padding mechanism is specified in ISO 9796 # 2.
USC+AXZ4711+4::541234500006:2+3'	The reference to the certificate issued by the trust centre identified with the GLN 5412345000006 is AXZ4711. The syntax of the certificate is X.509.
USA+6:16:1:10:1:7:1'	The algorithm used for generating the signature is RSA, the padding mechanism is specified in ISO 9796 # 2.
USB+1++5412345678908:14+8798765432106:14'	The sender and recipient of the interchange in which the AUTACK is present are identified with the GLNs 5412345678908 and 8798765432106.

6. Examples

USX+INT12436+5412345678908:14+8798765432106:14++++ME0001'	The first referenced message ME0001 to which security functions were applied is within interchange INT12346. The sender and recipient of the interchange in which the referenced message is present are identified with the GLNs 5412345678908 and 8798765432106.
USY+1+1:139B7CB7.....C72B03CE5F'	The digital signature of the first message is 139B7CB.....7C72B03CE5F.
USX+INT12436+5412345678908:14+8798765432106:14++++ME0002'	The second referenced message ME0002 to which security functions were applied is within interchange INT12346. The sender and recipient of the interchange in which the referenced message is present are identified with the GLNs 5412345678908 and 8798765432106.
USY+1+1:145D8BB.....2B69B38DC6A'	The digital signature of the second message is 145D8BB.....2B69B38DC6A.
USX+INT12436+5412345678908:14+8798765432106:14++++ME0003'	The third referenced message ME0003 to which security functions were applied is within interchange INT12346. The sender and recipient of the interchange in which the referenced message is present are identified with the GLNs 5412345678908 and 8798765432106.
USY+1+1:186A3DC.....4C54B59CE4E'	The digital signature of the third message is 186A3DC.....4C54B59CE4E.
UST+1+5'	The number of security segments in the segment groups 1, 2 and 4 equals 5.
UNT+14+AUT0001'	Message trailer, the total number of segments equals 14.
UNZ+4+12346'	Interchange trailer