EANCOM 2002 Syntax 4

Edition 2016_Update 2021

Secure Authentification - Acknowledgement (AUTACK)

Introduction

The following message specification is based on the publication of the "Secure Authentification - Acknowledgement Message" of GS1 Global in syntax 4.

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

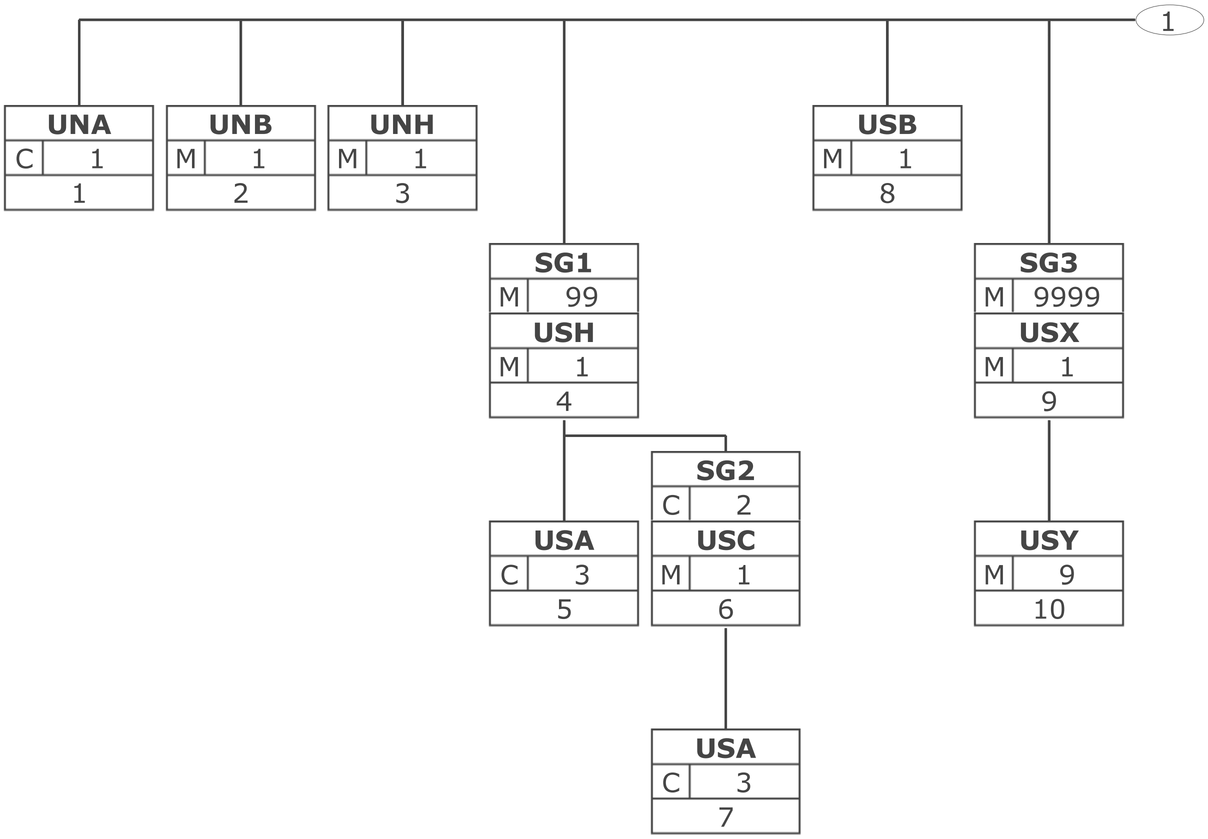
The applied security procedures shall be agreed to by trading partners and specified in an interchange agreement. The secure authentication and acknowledgement message (AUTACK) applies security services to other EDIFACT structures (messages, packages, groups or interchanges). It can be applied to combinations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

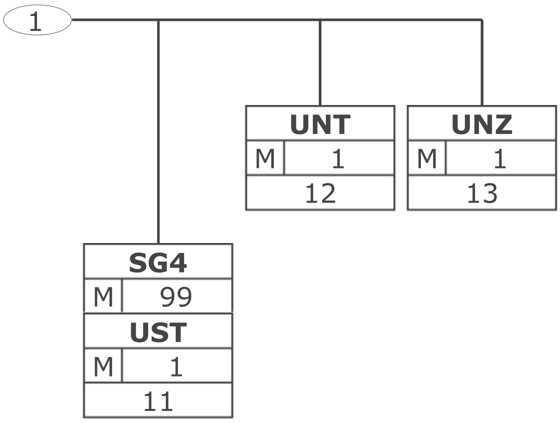
An AUTACK message used as an authentication message shall be sent by the originator of one or more other EDIFACT structures, or by a party having authority to act on behalf of the originator. Its purpose is to facilitate the security services provided by electronic signatures, i.e., authenticity, integrity,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

Branching Diagram



Tag		Tag = Segment/Group Tag
St	MaxOcc	St = Status (M=Mandatory, C=Conditional, R=Required, O=Optional, A=Advised, D=Dependent)
No		MaxOcc = Maximum occurrence of the segment/group; No = Consecutive segment number

Branching Diagram



Tag	
St	MaxOcc
No	

Tag = Segment/Group Tag
St = Status (M=Mandatory, C=Conditional, R=Required, O=Optional, A=Advised, D=Dependent)
MaxOcc = Maximum occurrence of the segment/group; No = Consecutive segment number

Message Structure

Seg.	No.	Status	Max Occ	Segment
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

Segment Layout

No.	Seg	St	Max. Occ.	
1	**UNA**	C	1	Service string advice

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.

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

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.

Example: `UNA:+.?*'`

Example: `UNA:+.?*'`

Max. Occ. = Maximum Occurrence, St = Status, * = Restricted Codes
Status: M=Mandatory, R=Required, O=Optional, C=Conditional, D=Dependent, A=Advised, N=Not used

Segment Layout

No.	Seg	St	Max. Occ.	
2	**UNB**	M	1	Interchange header

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.

Business Term	DE	EDIFACT	Format	St	*	Description
	S001	Syntax identifier		M		See Part I chapter 5.2.7 and segment notes.
	0001	Syntax identifier	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	an1	M	*	4 Version 4
	S002	Interchange sender		M		
	0004	Interchange sender identification	an..35	M		GLN (n13)
	0007	Identification code qualifier	an..4	R	*	14 GS1
	0008	Interchange sender internal identification	an..35	O		
	S003	Interchange recipient		M		
	0010	Interchange recipient identification	an..35	M		GLN (n13)
	0007	Identification code qualifier	an..4	R	*	14 GS1
	0014	Interchange recipient internal identification	an..35	O		
	S004	Date and time of preparation		M		
	0017	Date	n8	M		CCYYMMDD
	0019	Time	n4	M		HHMM
	0020	Interchange control reference	an..14	M		Unique reference identifying the interchange. Created by the interchange sender.
	S005	Recipient reference/ password details		O		

Max. Occ. = Maximum Occurrence, St = Status, * = Restricted Codes
Status: M=Mandatory, R=Required, O=Optional, C=Conditional, D=Dependent, A=Advised, N=Not used

Segment Layout

Business Term	DE	EDIFACT	Format	St	*	Description
	0022	Recipient reference/ password	an..14	M		
	0025	Recipient reference/ password qualifier	an2	O		
	0026	Application reference	an..14	O		Message identification if the interchange contains only one type of message.
	0029	Processing priority code	a1	O		A Highest priority
	0031	Acknowledgement request	n1	O		1 Requested
	0032	Interchange agreement identifier	an..35	O	*	EANCOM......
	0035	Test indicator	n1	O		1 Interchange is a test

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

Max. Occ. = Maximum Occurrence, St = Status, * = Restricted Codes
Status: M=Mandatory, R=Required, O=Optional, C=Conditional, D=Dependent, A=Advised, N=Not used

Segment Layout

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 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.

Example: `UNB+UNOA:4+4012345000009:14:1+4000004000002:14:4000004000099+20151013:1043+12345555+REF:AA++A+1+EANCOM-DISI+1'`

Example: `UNB+UNOC:4+5412345678908:14+8798765432106:14+20020102:1000+12345555+++++EANCOMREF52'`

Segment Layout

No.	Seg	St	Max. Occ.	
3	**UNH**	M	1	Message header

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.

Business Term	DE	EDIFACT	Format	St	*	Description
	0062	Message reference number	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		
	0065	Message type	an..6	M	*	AUTACK
	0052	Message version number	an..3	M	*	4 Service message, version 4
	0054	Message release number	an..3	M	*	1 First release
	0051	Controlling agency, coded	an..3	M	*	UN UN/CEFACT
	0057	Association assigned code	an..6	R	*	EAN001 GS1 version control number (GS1 Permanent Code)
	0110	Code list directory version number	an..6	O		

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:

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

Max. Occ. = Maximum Occurrence, St = Status, * = Restricted Codes
Status: M=Mandatory, R=Required, O=Optional, C=Conditional, D=Dependent, A=Advised, N=Not used

Segment Layout

No.	Seg	St	Max. Occ.	
	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).

No.	Seg	St	Max. Occ.	
4	**USH**	M	1	Security header

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.

Business Term	DE	EDIFACT	Format	St	*	Description
	0501	Security service, coded	an..3	M	*	7 Referenced EDIFACT structure non-repudiation of origin
	0534	Security reference number	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	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.
		Response type, coded				

Segment Layout

Business Term	DE	EDIFACT	Format	St	*	Description
	0503		an..3	N		
	0505	Filter function, coded	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	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	an..3	N		
	S500	Security identification details		N		
	0577	Security party qualifier	an..3			
	0520	Security sequence number	an..35	N		
	S501	Security date and time		R		
	0517	Date and time qualifier	an..3	M	*	1 Security Timestamp Date and time when the signature was generated.
	0338	Event date	n..8	R		Date of event, format is CCYYMMDD.
	0314	Event time	an..15	R		Time of event, format is HHMMSS
	0336	Time offset	n4	O		UTC (Universal Co-ordinated Time) offset from event time. Format is HHMM. Shall be

Max. Occ. = Maximum Occurrence, St = Status, * = Restricted Codes
Status: M=Mandatory, R=Required, O=Optional, C=Conditional, D=Dependent, A=Advised, N=Not used

Segment Layout

Business Term	DE	EDIFACT	Format	St	*	Description
						prefixed with '-' for negative offsets.

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:

Example: `USH+7+1+3++2+1++++1:20011017:110522:0100'`
Example: `USH+7+1+3+1+2+1++++1:20011010:110522:0100'`

Max. Occ. = Maximum Occurrence, St = Status, * = Restricted Codes
Status: M=Mandatory, R=Required, O=Optional, C=Conditional, D=Dependent, A=Advised, N=Not used

Segment Layout

No.	Seg	St	Max. Occ.	
	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).

No.	Seg	St	Max. Occ.	
5	**USA**	C	3	Security algorithm

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.

Business Term	DE	EDIFACT	Format	St	*	Description
	S502	Security algorithm		M		
	0523	Use of algorithm, coded	an..3	M	*	1 Owner hashing
	0525	Cryptographic mode of operation, coded	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	an..3	R	*	1 UN/CEFACT
	0527	Algorithm, coded	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	an..3	R	*	1 UN/CEFACT
	0591	Padding mechanism, coded	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.

Max. Occ. = Maximum Occurrence, St = Status, * = Restricted Codes
Status: M=Mandatory, R=Required, O=Optional, C=Conditional, D=Dependent, A=Advised, N=Not used

Segment Layout

Business Term	DE	EDIFACT	Format	St	*	Description
	0601	Padding mechanism code list identifier	an..3	R	*	1 UN/CEFACT

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:

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

Max. Occ. = Maximum Occurrence, St = Status, * = Restricted Codes
Status: M=Mandatory, R=Required, O=Optional, C=Conditional, D=Dependent, A=Advised, N=Not used

Segment Layout

No. Seg St Max. Occ.

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).

SG2 C 2 USC-USA

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

6 **USC** M 1 Certificate

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.

Business Term	DE	EDIFACT	Format	St	*	Description
	0536	Certificate reference	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		R		

Max. Occ. = Maximum Occurrence, St = Status, * = Restricted Codes
Status: M=Mandatory, R=Required, O=Optional, C=Conditional, D=Dependent, A=Advised, N=Not used

Segment Layout

Business Term	DE	EDIFACT	Format	St	*	Description
	0577	Security party qualifier	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	an..35	O		Identification of the public key to verify the digital signature by the recipient.
	0511	Security party identification	an..51	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	an..3	D	*	2 GS1 ZZZ Mutually agreed
	0545	Certificate syntax and version, coded	an..3	D		3 X.509 Where it is decided to refer to a non-EDIFACT 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.

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:
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'

Example: `USC+AXZ4711+3:PUBLIC KEY:5412345000006:2+3'`
Example: `USC+AXZ4711+4::5412345000006:2+3'`

Segment Layout

No.	Seg	St	Max. Occ.	
	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).

No.	Seg	St	Max. Occ.	
	SG2	C	2	USC-USA

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

No.	Seg	St	Max. Occ.	
7	**USA**	C	3	Security algorithm

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.

Business Term	DE	EDIFACT	Format	St	*	Description
	S502	Security algorithm		M		
	0523	Use of algorithm, coded	an..3	M	*	6 Owner signing
	0525	Cryptographic mode of operation, coded	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	an..3	R	*	1 UN/CEFACT
	0527	Algorithm, coded	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	an..3	R	*	1 UN/CEFACT
	0591	Padding mechanism, coded	an..3	R	*	7 ISO 9796 #2 padding Note: "ISO 9796 #2 padding" specifies the technical standard which is facilitating the security service "digital

Max. Occ. = Maximum Occurrence, St = Status, * = Restricted Codes
Status: M=Mandatory, R=Required, O=Optional, C=Conditional, D=Dependent, A=Advised, N=Not used

Segment Layout

Business Term	DE	EDIFACT	Format	St	*	Description
						signature scheme giving message recovery" specified in DE 0525.
	0601	Padding mechanism code list identifier	an..3	R	*	1 UN/CEFACT

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:

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

Max. Occ. = Maximum Occurrence, St = Status, * = Restricted Codes
Status: M=Mandatory, R=Required, O=Optional, C=Conditional, D=Dependent, A=Advised, N=Not used

Segment Layout

No.	Seg	St	Max. Occ.	
8	**USB**	M	1	Secured data identification
	To contain details related to the AUTACK.			

Business Term	DE	EDIFACT	Format	St	*	Description
	0503	Response type, coded	an..3	M	*	1 No acknowledgement required
	S501	Security date and time		N		
	0517	Date and time qualifier	an..3			
	S002	Interchange sender		M		
	0004	Interchange sender identification	an..35	M		For identification of parties it is recommended to use GLN - Format n13.
	0007	Identification code qualifier	an..4	R	*	14 GS1
	S003	Interchange recipient		M		
	0010	Interchange recipient identification	an..35	M		For identification of parties it is recommended to use GLN - Format n13.
	0007	Identification code qualifier	an..4	R	*	14 GS1

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:

Example: `USB+1++ABSENDER-ID:14+EMPFAENGER-ID:14'`
Example: `USB+1++5412345123450:14+5411234512300:14'`

Max. Occ. = Maximum Occurrence, St = Status, * = Restricted Codes
Status: M=Mandatory, R=Required, O=Optional, C=Conditional, D=Dependent, A=Advised, N=Not used

Segment Layout

No.	Seg	St	Max. Occ.	
	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.			
9	**USX**	M	1	Security references
	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			

Business Term	DE	EDIFACT	Format	St	*	Description
	0020	Interchange control reference	an..14	M		Unique reference number of interchange containing the data to which the security service was applied (UNB, DE 0020).
	S002	Interchange sender		R		
	0004	Interchange sender identification	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	an..4	R	*	14 GS1
	S003	Interchange recipient		R		
	0010	Interchange recipient identification	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	an..4	R	*	14 GS1
	0048	Group reference number	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		N		
	0040	Application sender identification	an..35			
	S007	Application recipient identification		N		
	0044	Application recipient identification	an..35			
	0062	Message reference number	an..14	D		Reference number of a message (UNH to UNT) to

Max. Occ. = Maximum Occurrence, St = Status, * = Restricted Codes
Status: M=Mandatory, R=Required, O=Optional, C=Conditional, D=Dependent, A=Advised, N=Not used

Segment Layout

Business Term	DE	EDIFACT	Format	St	*	Description
						which the security service was applied (UNH, DE 0062 of this message).

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.
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:

Example: `USX+DAT REFERENZ+ABSENDER-ID:14+EMPFAENGER-ID:14+GRP REFERENZ+++MES REFERENZ'`
Example: `USX+DAT001+5412345123450:14+5411234512300:14+GRP002+++MES003'`

Segment Layout

No.	Seg	St	Max. Occ.	
	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.			
10	**USY**	M	9	Security on references
	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			

Business Term	DE	EDIFACT	Format	St	*	Description
	0534	Security reference number	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		R		
	0563	Validation value, qualifier	an..3	M	*	1 Unique validation value
	0560	Validation value	an..51	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.

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:

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

Max. Occ. = Maximum Occurrence, St = Status, * = Restricted Codes
Status: M=Mandatory, R=Required, O=Optional, C=Conditional, D=Dependent, A=Advised, N=Not used

Segment Layout

No.	Seg	St	Max. Occ.	
	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.			
11	**UST**	M	1	Security trailer

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.

Business Term	DE	EDIFACT	Format	St	*	Description
	0534	Security reference number	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	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.

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

Example: `UST+1+5'`

Example: `UST+1+5'`

Segment Layout

No.	Seg	St	Max. Occ.	
12	**UNT**	M	1	Message trailer

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.

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

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

Example: `UNT+10+AUT00001'`
Example: `UNT+10+AUT00001'`

Max. Occ. = Maximum Occurrence, St = Status, * = Restricted Codes
Status: M=Mandatory, R=Required, O=Optional, C=Conditional, D=Dependent, A=Advised, N=Not used

Segment Layout

No.	Seg	St	Max. Occ.	
13	**UNZ**	M	1	Interchange trailer

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.

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

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.

Example: `UNZ+1+12345555'`
Example: `UNZ+5+12345555'`

Used Codes

0001 Syntax identifier

Coded identification of the agency controlling the syntax, and of the character repertoire used in an interchange.

Notes:
1. The data value consists of the letters 'UN', upper case, identifying the syntax controlling agency, directly followed by an a2 code identifying the character repertoire used.

UNOA UN/ECE level A

As defined in the basic code table of ISO 646 with the exceptions of lower case letters, alternative graphic character allocations and national or application-oriented graphic character allocations.

UNOB UN/ECE level B

As defined in the basic code table of ISO 646 with the exceptions of alternative graphic character allocations and national or application-oriented graphic character allocations.

UNOC UN/ECE level C

As defined in ISO 8859-1 : Information processing - Part 1: Latin alphabet No. 1.

UNOD UN/ECE level D

As defined in ISO 8859-2 : Information processing - Part 2: Latin alphabet No. 2.

UNOE UN/ECE level E

As defined in ISO 8859-5 : Information processing - Part 5: Latin/Cyrillic alphabet.

UNOF UN/ECE level F

As defined in ISO 8859-7 : Information processing - Part 7: Latin/Greek alphabet.

UNOG UN/ECE level G

As defined in ISO 8859-3 : Information processing - Part 3: Latin alphabet.

UNOH UN/ECE level H

As defined in ISO 8859-4 : Information processing - Part 4: Latin alphabet.

UNOI UN/ECE level I

As defined in ISO 8859-6 : Information processing - Part 6: Latin/Arabic alphabet.

UNOJ UN/ECE level J

As defined in ISO 8859-8 : Information processing - Part 8: Latin/Hebrew alphabet.

UNOK UN/ECE level K

As defined in ISO 8859-9 : Information processing - Part 9: Latin alphabet.

Used Codes

UNOW	UN/ECE level W ISO 10646-1 octet with code extension technique to support UTF-8 (UCS Transformation Format, 8 bit) encoding.
UNOX	UN/ECE level X Code extension technique as defined by ISO 2022 utilising the escape techniques in accordance with ISO 2375.
UNOY	UN/ECE level Y ISO 10646-1 octet without code extension technique.
0002	Syntax version number Version number of the syntax. Notes: 1. Shall be '4' to indicate this version of the syntax.
4	Version 4 ISO 9735:1998.
0007	Identification code qualifier Qualifier referring to the identification code. Notes: 1. A qualifier code may refer to an organisation identification as in ISO 6523.
14	GS1 Partner identification code assigned by GS1, an international organization of GS1 Member Organizations that manages the GS1 System.
0025	Recipient reference/password qualifier Qualifier for the recipient's reference or password. Notes: 1. To be used as specified in the partners' interchange agreement.
AA	Reference Recipient's reference/password is a reference.
BB	Password Recipient's reference/password is a password.
0029	Processing priority code Code determined by the sender requesting processing priority for the interchange. Notes: 1. To be used as specified in the partners' interchange agreement.

A	Highest priority Requested processing priority is the highest.
0031	Acknowledgement request Code requesting acknowledgement for the interchange. Notes: 1. Used if the sender requests that a message related to syntactical correctness be sent by the recipient in response. 2. For UN/EDIFACT a specific message (Syntax and service report - CONTRL) is defined for this purpose.
1	Requested Acknowledgement is requested.
0035	Test indicator Indication that the structural level containing the test indicator is a test.
1	Interchange is a test Indicates that the interchange is a test.
5	Interchange is a service provider test Indicates that this interchange is a test with a service provider.
0051	Controlling agency, coded Code identifying a controlling agency.
AA	EDICONSTRUCT French construction project.
AB	DIN (Deutsches Institut fuer Normung) German standardization institute.
AC	ICS (International Chamber of Shipping) The International Chamber of Shipping.
AD	UPU (Union Postale Universelle) Universal Postal Union.
AE	United Kingdom ANA (Article Numbering Association) Identifies the Article Numbering Association of the United Kingdom.
AF	ANSI ASC X12 (American National Standard Institute Accredited Standards Committee X12) Identifies the United States electronic data interchange standards body.
AG	US DoD (United States Department of Defense) The United States Department of Defense is the entity controlling the message specification.

Used Codes

AH	US Federal Government The United States Federal Government is the entity controlling the message specification.
AI	EDIFICAS European EDI association for financial, informational, cost, accounting, auditing and social areas.
AJ	UN/ECE/TRANS United Nations Economic Commission for Europe (UN/ECE), Sustainable Transport Division (TRANS)
CC	CCC (Customs Co-operation Council) The Customs Co-operation Council.
CE	CEFIC (Conseil Europeen des Federations de l'Industrie Chimique) EDI project for chemical industry.
EC	EDICON UK Construction project.
ED	EDIFICE (Electronic industries project) EDI Forum for companies with Interest in Computing and Electronics (EDI project for EDP/ADP sector).
EE	EC + EFTA (European Communities and European Free Trade Association) The European Communities and the European Free Trade Association.
EN	GS1 Partner identification code assigned by GS1, an international organization of GS1 Member Organizations that manages the GS1 System.
ER	UIC (International Union of railways) European railways.
EU	European Union The European Union.
EW	UN/EDIFACT Working Group (EWG) United Nations working group responsible for UN/EDIFACT (United Nations, Electronic Data Interchange for Administration, Commerce and Transport).
EX	IECC (International Express Carriers Conference) The International Express Carriers Conference.
IA	IATA (International Air Transport Association) The International Air Transport Association.
KE	KEC (Korea EDIFACT Committee) The Korea EDIFACT Committee.
LI	LIMNET UK Insurance project.

Used Codes

OD	ODETTE (Organization for Data Exchange through Tele-Transmission in Europe) European automotive industry project.
RI	RINET (Reinsurance and Insurance Network) The Reinsurance and Insurance Network.
RT	UN/ECE/TRADE/WP.4/GE.1/EDIFACT Rapporteurs' Teams United Nations Economic UN Economic Commission for Europe (UN/ECE), Committee on the development of trade (TRADE), Working Party on facilitation of international trade procedures (WP.4), Group of Experts on data elements and automatic data interchange (GE.1), EDIFACT Rapporteurs' Teams.
UN	UN/CEFACT United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT). GS1 Description: UN Economic Commission for Europe (UN/ECE), Committee on the development of trade (TRADE), Working Party on facilitation of international trade procedures (WP.4).

0052

Message version number

Version number of a message type.

1	Status 1 version Message approved and issued as a status 1 (trial) message. (Valid for directories published after March 1990 and prior to March 1993).
2	Status 2 version Message approved and issued as a status 2 (formal recommendation) message. (Valid for directories published after March 1990 and prior to March 1993).
4	Service message, version 4 Service messages approved and issued as a part of ISO 9735/Version 4, for use with that version of the syntax. Notes: For earlier versions of the UN/EDIFACT CONTRL message, each published by the UN as a stand-alone message, the version number to be used is specified in the message documentation.
88	1988 version Message approved and issued in the 1988 release of the UNTDID (United Nations Trade Data Interchange Directory) as a status 2 (formal recommendation) message.
89	1989 version Message approved and issued in the 1989 release of the UNTDID (United Nations Trade Data Interchange Directory) as a status 2 (formal recommendation) message.

90

1990 version

Message approved and issued in the 1990 release of the UNTDID (United Nations Trade Data Interchange Directory) as a status 2 (formal recommendation) message.

D

Draft version/UN/EDIFACT Directory

Message approved and issued as a draft message (Valid for directories published after March 1993 and prior to March 1997). Message approved as a standard message (Valid for directories published after March 1997).

S

Standard version

Message approved and issued as a standard message. (Valid for directories published after March 1993 and prior to March 1997).

0054

Message release number

Release number within the current message version number.

1

First release

Message approved and issued in the first release of the year of the UNTDID (United Nations Trade Data Interchange Directory).

2

Second release

User message approved and issued in the second release of the year of the UNTDID (United Nations Trade Data Interchange Directory); valid for directories published prior to March 1990. Service message approved and issued as the second release of the message within a version of ISO 9735; valid for version 4 of IS0 9735 and later.

902

Trial release 1990

Message approved and issued in the 1990 status 1 (trial) release of the UNTDID (United Nations Trade Data Interchange Directory).

911

Trial release 1991

Message approved and issued in the 1991 status 1 (trial) release of the UNTDID (United Nations Trade Data Interchange Directory).

912

Standard release 1991

Message approved and issued in the 1991 status 2 (standard) release of the UNTDID (United Nations Trade Data Interchange Directory).

921

Trial release 1992

Message approved and issued in the 1992 status 1 (trial) release of the UNTDID (United Nations Trade Data Interchange Directory).

932

Standard release 1993

Message approved and issued in the 1993 status 2 (standard) release of the UNTDID (United Nations Trade Data Interchange Directory).

00A

Release 2000 - A

Message approved and issued in the first 2000 release of the UNTDID (United Nations Trade Data Interchange Directory).

Used Codes

00B	Release 2000 - B Message approved and issued in the second 2000 release of the UNTDID (United Nations Trade Data Interchange Directory).
01A	Release 2001 - A Message approved and issued in the first 2001 release of the UNTDID (United Nations Trade Data Interchange Directory).
01B	Release 2001 - B Message approved and issued in the second 2001 release of the UNTDID (United Nations Trade Data Interchange Directory).
01C	Release 2001 - C Message approved and issued in the third 2001 release of the UNTDID (United Nations Trade Data Interchange Directory).
02A	Release 2002 - A Message approved and issued in the first 2002 release of the UNTDID (United Nations Trade Data Interchange Directory).
02B	Release 2002 - B Message approved and issued in the second 2002 release of the UNTDID (United Nations Trade Data Interchange Directory).
03A	Release 2003 - A Message approved and issued in the first 2003 release of the UNTDID (United Nations Trade Data Interchange Directory).
03B	Release 2003 - B Message approved and issued in the second 2003 release of the UNTDID (United Nations Trade Data Interchange Directory).
04A	Release 2004 - A Message approved and issued in the first 2004 release of the UNTDID (United Nations Trade Data Interchange Directory).
04B	Release 2004 - B Message approved and issued in the second 2004 release of the UNTDID (United Nations Trade Data Interchange Directory).
05A	Release 2005 - A Message approved and issued in the first 2005 release of the UNTDID (United Nations Trade Data Interchange Directory).
05B	Release 2005 - B Message approved and issued in the second 2005 release of the UNTDID (United Nations Trade Data Interchange Directory).
06A	Release 2006 - A Message approved and issued in the first 2006 release of the UNTDID (United Nations Trade Data Interchange Directory).

Used Codes

06B	Release 2006 - B Message approved and issued in the second 2006 release of the UNTDID (United Nations Trade Data Interchange Directory).
07A	Release 2007 - A Message approved and issued in the first 2007 release of the UNTDID (United Nations Trade Data Interchange Directory).
07B	Release 2007 - B Message approved and issued in the second 2007 release of the UNTDID (United Nations Trade Data Interchange Directory).
08A	Release 2008 - A Message approved and issued in the first 2008 release of the UNTDID (United Nations Trade Data Interchange Directory).
08B	Release 2008 - B Message approved and issued in the second 2008 release of the UNTDID (United Nations Trade Data Interchange Directory).
09A	Release 2009 - A Message approved and issued in the first 2009 release of the UNTDID (United Nations Trade Data Interchange Directory).
09B	Release 2009 - B Message approved and issued in the second 2009 release of the UNTDID (United Nations Trade Data Interchange Directory).
10A	Release 2010 - A Message approved and issued in the first 2010 release of the UNTDID (United Nations Trade Data Interchange Directory).
10B	Release 2010 - B Message approved and issued in the second 2010 release of the UNTDID (United Nations Trade Data Interchange Directory).
11A	Release 2011 - A Message approved and issued in the first 2011 release of the UNTDID (United Nations Trade Data Interchange Directory).
11B	Release 2011 - B Message approved and issued in the second 2011 release of the UNTDID (United Nations Trade Data Interchange Directory).
12A	Release 2012 - A Message approved and issued in the first 2012 release of the UNTDID (United Nations Trade Data Interchange Directory).
12B	Release 2012 - B Message approved and issued in the second 2012 release of the UNTDID (United Nations Trade Data Interchange Directory).

Used Codes

13A	Release 2013 - A Message approved and issued in the first 2013 release of the UNTDID (United Nations Trade Data Interchange Directory).
13B	Release 2013 - B Message approved and issued in the second 2013 release of the UNTDID (United Nations Trade Data Interchange Directory).
14A	Release 2014 - A Message approved and issued in the first 2014 release of the UNTDID (United Nations Trade Data Interchange Directory).
14B	Release 2014 - B Message approved and issued in the second 2014 release of the UNTDID (United Nations Trade Data Interchange Directory).
15A	Release 2015 - A Message approved and issued in the first 2015 release of the UNTDID (United Nations Trade Data Interchange Directory).
15B	Release 2015 - B Message approved and issued in the second 2015 release of the UNTDID (United Nations Trade Data Interchange Directory).
16A	Release 2016 - A Message approved and issued in the first 2016 release of the UNTDID (United Nations Trade Data Interchange Directory).
16B	Release 2016 - B Message approved and issued in the second 2016 release of the UNTDID (United Nations Trade Data Interchange Directory).
17A	Release 2017 - A Message approved and issued in the first 2017 release of the UNTDID (United Nations Trade Data Interchange Directory).
17B	Release 2017 - B Message approved and issued in the second 2017 release of the UNTDID (United Nations Trade Data Interchange Directory).
18A	Release 2018 - A Message approved and issued in the first 2018 release of the UNTDID (United Nations Trade Data Interchange Directory).
18B	Release 2018 - B Message approved and issued in the second 2018 release of the UNTDID (United Nations Trade Data Interchange Directory).
19A	Release 2019 - A Message approved and issued in the first 2019 release of the UNTDID (United Nations Trade Data Interchange Directory).

Used Codes

19B	Release 2019 - B Message approved and issued in the second 2019 release of the UNTDID (United Nations Trade Data Interchange Directory).
20A	Release 2020 - A Message approved and issued in the first 2020 release of the UNTDID (United Nations Trade Data Interchange Directory).
20B	Release 2020 - B Message approved and issued in the second 2020 release of the UNTDID (United Nations Trade Data Interchange Directory).
21A	Release 2021 - A Message approved and issued in the first 2021 release of the UNTDID (United Nations Trade Data Interchange Directory).
21B	Release 2021 - B Message approved and issued in the second 2021 release of the UNTDID (United Nations Trade Data Interchange Directory).
93A	Release 1993 - A Message approved and issued in the 1993 release of the UNTDID (United Nations Trade Data Interchange Directory).
94A	Release 1994 - A Message approved and issued in the first 1994 release of the UNTDID (United Nations Trade Data Interchange Directory).
94B	Release 1994 - B Message approved and issued in the second 1994 release of the UNTDID (United Nations Trade Data Interchange Directory).
95A	Release 1995 - A Message approved and issued in the first 1995 release of the UNTDID (United Nations Trade Data Interchange Directory).
95B	Release 1995 - B Message approved and issued in the second 1995 release of the UNTDID (United Nations Trade Data Interchange Directory).
96A	Release 1996 - A Message approved and issued in the first 1996 release of the UNTDID (United Nations Trade Data Interchange Directory).
96B	Release 1996 - B Message approved and issued in the second 1996 release of the UNTDID (United Nations Trade Data Interchange Directory).
97A	Release 1997 - A Message approved and issued in the first 1997 release of the UNTDID (United Nations Trade Data Interchange Directory).

Used Codes

97B	Release 1997 - B Message approved and issued in the second 1997 release of the UNTDID (United Nations Trade Data Interchange Directory).
98A	Release 1998 - A Message approved and issued in the first 1998 release of the UNTDID (United Nations Trade Data Interchange Directory).
98B	Release 1998 - B Message approved and issued in the second 1998 release of the UNTDID (United Nations Trade Data Interchange Directory).
99A	Release 1999 - A Message approved and issued in the first 1999 release of the UNTDID (United Nations Trade Data Interchange Directory).
99B	Release 1999 - B Message approved and issued in the second 1999 release of the UNTDID (United Nations Trade Data Interchange Directory).

0057	Association assigned code Code, assigned by the association responsible for the design and maintenance of the message type concerned, which further identifies the message.
EAN001	GS1 version control number (GS1 Permanent Code) Indicates that the message is an EANCOM message in version 001.

0065	Message type Code identifying a type of message and assigned by its controlling agency. Notes: 1. In UNSMs (United Nations Standard Messages), the representation is a6.
AUTACK	

0501	Security service, coded Specification of the security service applied.
7	Referenced EDIFACT structure non-repudiation of origin The referenced EDIFACT structure is secured by a digital signature protecting the receiver of the message from the sender's denial of having sent the message.

0503	Response type, coded Specification of the type of response expected from the recipient.
1	No acknowledgement required No AUTACK acknowledgement message expected.

Used Codes

0505	Filter function, coded Identification of the filtering function used to reversibly map any bit pattern on to a restricted character set.
2	Hexadecimal filter Hexadecimal filter.

0507	Original character set encoding, coded Identification of the character set in which the secured EDIFACT structure was encoded when security mechanisms were applied.
1	ASCII 7 bit ASCII 7 bit code.
2	ASCII 8 bit ASCII 8 bit code.
3	Code page 850 (IBM PC Multinational) Encoding schema for the repertoire as defined by the code page.
4	Code page 500 (EBCDIC Multinational No. 5) Encoding schema for the repertoire as defined by the code page.

0513	Security party code list qualifier Identification of the type of identification used to register the security parties.
2	GS1 GS1, an international organization of GS1 Member Organizations that manages the GS1 System.
ZZZ	Mutually agreed Mutually agreed between trading partners.

0517	Date and time qualifier Specification of the type of date and time.
1	Security Timestamp Security timestamp of the secured message.
2	Certificate generation date and time Identifies the date and time of generation of the certificate by the Certification Authority.
3	Certificate start of validity period Identifies the date and time from which the certificate must be considered valid.
4	Certificate end of validity period Identifies the date and time until which the certificate must be considered valid.

Used Codes

5	EDIFACT structure generation date and time Date and time of generation of the secured EDIFACT structure.
6	Certificate revocation date and time Identifies the date and time of revocation of the certificate by the Certification Authority.
7	Key generation date and time Identifies the date and time of generation of the key(s).
0523	Use of algorithm, coded Specification of the usage made of the algorithm.
1	Owner hashing Specifies that the algorithm is used by the message sender to compute the hash function on the message (as in the case of Integrity or Non-repudiation of Origin identified in the security function qualifier of USH).
6	Owner signing Specifies that the algorithm is used by the message sender to sign either the hash result computed on the message or the symmetric keys.
0525	Cryptographic mode of operation, coded Specification of the mode of operation used for the algorithm.
16	DSMR Digital Signature scheme giving Message Recovery. ISO 9796.
0527	Algorithm, coded Identification of the algorithm.
1	DES Data Encryption Standard. FIPS Pub 46 (January 1977).
2	MAA Message Authentication Algorithm. Banking-Approved Algorithms for message Authentication. ISO 8731-2.
3	FEAL FEAL Fast Data Encipherment Algorithm.
4	IDEA International Data Encryption Algorithm: Lai X., Massey J. ""A Proposal for a New Block Encryption Standard"", Proceedings of Eurocrypt'90, LNCS vol 473, Springer-Verlag, Berlin 1991, and Lai X., Massey J. ""Markov Ciphers and Differential Cryptanalysis"", Proceedings of Eurocrypt'91, LNCS vol 547, Springer-Verlag, Berlin 1991.
5	MD4 The MD4 Message digest algorithm. Rivest R. RSA Data Security Inc. (1990).

Used Codes

6	MD5 The MD5 Message digest algorithm. Rivest R. Dusse S. RSA Data Security Inc. (1991).
7	RIPEMD Extension of the MD4 - Ripe Report CS - R9324, April 93.
8	SHA Secure Hashing Algorithm.
9	AR/DFP Hash function of the German banking industry, submitted to ISO/IEC JTC 1/SC 27/WG 2, Doc N179.
10	RSA Rivest, Shamir, Adleman: A Method for obtaining Digital Signatures and Public Key Cryptosystems. Communications of the ACM, Vol.21(2), pp 120-126 (1978).
11	DSA Digital Signature Algorithm/Digital Signature Standard NIST Pub 1993 Draft.
12	RAB Rabin, "Digitalized signatures and public-key functions as intractable as factorization", MIT Laboratory for Computer Science Technical Report LCS/TR-212, Cambridge, Mass, 1979.
13	TDEA Triple Data Encryption Algorithm; ANSI X9.52.
14	RIPEMD-160 Dedicated Hash-Function #1; ISO 10118-3.
15	RIPEMD-128 Dedicated Hash-Function #2; ISO/IEC 10118-3.
16	SHA1 Secure Hash Algorithm, dedicated Hash-Function #3; ISO 10118-3.
17	ECC Elliptic Curve Algorithm, Draft IEEE P1363 standard.
18	ZLIB Data compression algorithm; Deflate/inflate algorithm published in RFC1950, RFC1951 and RFC1952.
20	INFOZIP Data compression algorithm.
21	OLZW Data compression algorithm; Optimized LZW; Published in 'Dr. Dobb's Journal' (Jun 1990).

Used Codes

22	ARITCODE Data compression algorithm; Arithmetic coding; Published in 'Comm. Of the ACM' (Jun 1987).
23	SHUFF Data compression algorithm; Static Huffman; Published in 'Proceedings of the I.R.E.' (Sep. 1952).
24	DHUFF Data compression algorithm; Dynamic Huffman; Published in 'ACM Transaction on Mathematical Software' (Jun 1989).
25	CRC-32 Cyclic Redundancy Check - 32-bit; Ethernet CRC.
26	CRC-CCITT Cyclic Redundancy Check - 16-bit.
27	ISO/IEC 12042 Data compression for information exchange - Binary arithmetic coding algorithm; ISO/IEC 12042.
28	RC4 Variable-Key Size Symmetric Stream Cipher, specified by RSA Security Inc.
29	RC5 Variable-Key Size Symmetric Block Cipher, published in RFC 2040.
30	HMAC-SHA1 Message Authentication using keyed SHA-1 (published in RFC 2104).
31	HMAC-MD5 Message Authentication using keyed MD5 (published in RFC 2104).
32	HMAC-RIPEMD-160 Messahe Authentication using keyed RIPEMD-160 (published in RFC 2104).
33	HMAC-RIPEMD-128 Message Authentication using keyed RIPEMD-128 (published in RFC 2104).
34	DB-MACv3 MAC calculation (variant 3), using RIPEMD-160 and triple DES (published by Deutsche Bundesbank 1998).
35	LZ77 Lempel Ziv, 1977 data compression algorithm.
36	LZW Lempel Ziv Welch data compression algorithm.
37	MAC-ISO 8731-1 Message authentication code defined in ISO 8731-1.

Used Codes

38	DIM1 Data integrity mechanism using a cryptographic check function; ISO/IEC 9797, first method.
39	DIM2 Data integrity mechanism using a cryptographic check function; ISO/IEC 9797, second method.
40	MDC2 Modification detection code, IBM System Journal, vol 13, #2, 1991.
41	HDS1 ISO/IEC 10118-1; hash functions using an n-bit block cipher algorithm providing a single length hash code.
42	HDS2 ISO/IEC 10118-1; hash functions using an n-bit block cipher algorithm providing a double length hash code.
43	SQM ISO/IEC 9594-8. Square-Mod-N hash function for RSA.
44	NVB 7.1 Dutch banking standard for hashing and signing using RSA.
45	PKCS#1-v2_MGF1 Mask Generation Function defined in PKCS#1, Version 2.
46	NVBAK Dutch banking standard, NVB Authenticity Mark, published by the NVB, May 1992.
47	MCCP Banking key management by means of asymmetric algorithms, algorithms using the RSA cryptosystem. Signature construction by means of a separate signature. ISO 11166-2.
48	SHA-256 Identification of the algorithm.
49	SHA-512 Secure Hash Algorithm, dedicated Hash-Function #5; ISO 10118-3.
50	SHA-384 Secure Hash Algorithm, dedicated Hash-Function #6; ISO 10118-3.
51	WHIRLPOOL Secure Hash Algorithm, dedicated Hash-Function #7; ISO 10118-3.
52	SHA-224 Secure Hash Algorithm standard issued by NIST (National Institute of Standards and Technology) in FIPS PUB 180-2 (Change Notice 1, 2004).

ZZZ	Mutually agreed Mutually agreed between trading partners.
0529	Algorithm code list identifier Specification of the code list used to identify the algorithm.
1	UN/CEFACT United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT).
0531	Algorithm parameter qualifier Specification of the type of parameter value.
1	Initialisation value, clear text Identifies the algorithm parameter value as an unencrypted initialisation value.
2	Initialisation value, encrypted under a symmetric key Identifies the algorithm parameter value as an initialisation value which is encrypted under the symmetric data key.
3	Initialisation value, encrypted under a public key Identifies the algorithm parameter value as an initialisation value encrypted under the public key of the receiving party.
4	Initialisation value, format mutually agreed Identifies the algorithm parameter value as an initialisation value in a format agreed between the two parties.
5	Symmetric key, encrypted under a symmetric key Identifies the algorithm parameter value as a symmetric key which is encrypted with a previously agreed algorithm under a previously exchanged symmetric key.
6	Symmetric key, encrypted under a public key Identifies the algorithm parameter value as a symmetric key encrypted under the public key of the receiving party.
7	Symmetric key, signed and encrypted Identifies the algorithm parameter value as a symmetric key signed under the sender's secret key, then encrypted under the receiver's public key.
8	Symmetric key encrypted under an asymmetric key common to the sender and the receiver Identifies the algorithm parameter value as a symmetric key encrypted under an asymmetric key common to the sender and the receiver (use of Diffie and Hellman scheme, for instance).
9	Symmetric key name Identifies the algorithm parameter value as the name of a symmetric key. This may be used in the case where a key relationship has already been established between the sender and receiver.

Used Codes

10	Key encrypting key name Identifies the parameter value as the name of a key encrypting key.
11	Symmetric key, format mutually agreed Identifies the algorithm parameter value as a symmetric key in a format agreed between the two parties.
12	Modulus Identifies the algorithm parameter value as the modulus of a public key which is to be used according to the function defined by the use of algorithm.
13	Exponent Identifies the algorithm parameter value as the exponent of a public key which is to be used according to the function defined by the use of algorithm.
14	Modulus length Identifies the algorithm parameter value as the length of the modulus (in bits) of the public key used in the algorithm. The length is independent of whatever filtering function may be in use.
15	Generic parameter 1 Identifies the algorithm parameter value as the first generic parameter.
16	Generic parameter 2 Identifies the algorithm parameter value as the second generic parameter.
17	Generic parameter 3 Identifies the algorithm parameter value as the third generic parameter.
18	Generic parameter 4 Identifies the algorithm parameter value as the fourth generic parameter.
19	Generic parameter 5 Identifies the algorithm parameter value as the fifth generic parameter.
20	Generic parameter 6 Identifies the algorithm parameter value as the sixth generic parameter.
21	Generic parameter 7 Identifies the algorithm parameter value as the seventh generic parameter.
22	Generic parameter 8 Identifies the algorithm parameter value as the eighth generic parameter.
23	Generic parameter 9 Identifies the algorithm parameter value as the ninth generic parameter.
24	Generic parameter 10 Identifies the algorithm parameter value as the tenth generic parameter.
25	DSA parameter P Identifies the algorithm parameter value as the parameter P of DSA algorithm.

Used Codes

26	DSA parameter Q Identifies the algorithm parameter value as the parameter Q of DSA algorithm.
27	DSA parameter G Identifies the algorithm parameter value as the parameter G of DSA algorithm.
28	DSA parameter Y Identifies the algorithm parameter value as the parameter Y of DSA algorithm.
29	Initial value for CRC calculation Identifies the algorithm parameter value as the initial value for the CRC calculation.
30	Initial directory tree Identifies the algorithm parameter value as the initial directory tree for the data compression algorithm specified.
31	Integrity value offset Identifies the algorithm parameter value as the offset within the compressed text where the integrity value is located.
33	Generator Identifies the algorithm parameter value as the generator for a secret key agreement mechanism.
34	Symmetric key activation date/time Identifies the activation date/time of a symmetric key. The date/time format shall be CCYYMMDDHHMMSS.
35	PKCS#1-EME-OAEP HF Identifies the algorithm parameter value as the code of the hash function used by EME-OAEP padding mechanism as defined in PKCS#1, Version 2.
36	PKCS#1-EME-OAEP MGF Identifies the algorithm parameter value as the code of the mask generation function used by EME-OAEP padding mechanism as defined in PKCS#1, Version 2.
37	PKCS#1-EME-OAEP P Init Identifies the algorithm parameter value as the initial octets of the encoding parameter octet string (P) used by EME-OAEP padding mechanism as defined in PKCS#1, Version 2.
38	PKCS#1-EME-OAEP P Cont Identifies the algorithm parameter value as the additional octets of the encoding parameter octet string (P) following the initial octets, used by EME-OAEP padding mechanism as defined in PKCS#1, Version 2.
39	PKCS#1-EME-OAEP P Final Identifies the algorithm parameter value as the final octets of the encoding parameter octet string (P) following the initial or additional octets, used by EME-OAEP padding mechanism as defined in PKCS#1, Version 2.

Used Codes

40	PKCS#1-EME-OAEP HF/MGF Identifies the algorithm parameter value as the code of the hash function used by the mask generation function used by EME-OAEP padding mechanism as defined in PKCS#1, Version 2.
41	PKCS#1-EME-OAEP LENGTH Identifies the algorithm parameter value as the intended length of the result produced by EME-OAEP padding mechanism as defined in PKCS#1, Version 2.
ZZZ	Mutually agreed Mutually agreed between trading partners.
0533	Mode of operation code list identifier Specification of the code list used to identify the cryptographic mode of operation.
1	UN/CEFACT United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT).
0541	Scope of security application, coded Specification of the scope of application of the security service defined in the security header. Notes: 1. It defines the data that have to be taken into account by the related cryptographic process.
3	Whole related message, package, group or interchange From the first character of the message, group, or interchange to the last character of the message, group or interchange.
6	Part related message, package, group or interchange (GS1 Temporary Code) From the first message header segment to the last message trailer segment
0545	Certificate syntax and version, coded Coded identification of the syntax and version used to create the certificate.
1	EDIFACT version 4 ISO 9735 version 4.
2	EDIFACT version 3 ISO 9735 version 3.
3	X.509 ISO/IEC 9594-8, ITU X.509 key/certificate reference.
4	PGP PGP (Pretty Good Privacy) based format key/certificate reference.

Used Codes

5	EDI 5 v1.4 Version 1.4 of the EDI 5 certificate (French national standard).
0551	Service character for signature qualifier Identification of the type of service character used when the signature was computed.
1	Segment terminator Specifies that this is the separator at the end of segments.
2	Component data element separator Specifies that this is the separator between component data elements.
3	Data element separator Specifies that this is the separator between data elements.
4	Release character Specifies that this is the release character.
5	Repetition separator Specifies that this is the separator between repeating data elements.
0563	Validation value, qualifier Identification of the type of validation value.
1	Unique validation value Specifies that this is the unique validation value. This code shall be used when the algorithm involved produces a single parameter result (one MAC with DES algorithm, or one digital signature with RSA algorithm, for instance).
0577	Security party qualifier Identification of the role of the security party.
1	Message sender Identifies the party which generates the security parameters of the message (i.e. security originator).
2	Message receiver Identifies the party which verifies the security parameters of the message (i.e. security recipient).
3	Certificate owner Identifies the party which owns the certificate.
4	Authenticating party Party which certifies that the document (i.e. the certificate) is authentic.
0591	Padding mechanism, coded Padding mechanism or padding scheme applied.

Used Codes

7	ISO 9796 #2 padding Message padding for digital signature schemes according to ISO 9796 part 2.
0601	Padding mechanism code list identifier Specification of the code list used to identify the padding mechanism or padding scheme.
1	UN/CEFACT United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT).

Example

```
UNA:+.?*'
    UNA:+.?*'
```

```
UNB+UNOA:4+4012345000009:14:1+4000004000002:14:4000004000099+20151013:10
43+12345555+REF:AA++A+1+EANCOM-DISI+1'
    UNB+UNOC:4+5412345678908:14+8798765432106:14+20020102:
    1000+12345555+++++EANCOMREF 52'
```

```
UNH+AUT00001+AUTACK:4:1:UN:EAN001:X'
    UNH+AUT00001+AUTACK:4:1:UN:EAN001'
```

```
USH+7+1+3++2+1++++1:20011017:110522:0100'
    USH+7+1+3+1+2+1++++1:20011010:110522:0100'
```

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

```
USC+AXZ4711+3:PUBLIC KEY:5412345000006:2+3'
    USC+AXZ4711+4::5412345000006:2+3'
```

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

```
USB+1++ABSENDER-ID:14+EMPFAENGER-ID:14'
    USB+1++5412345123450:14+5411234512300:14'
```

```
USX+DAT REFERENZ+ABSENDER-ID:14+EMPFAENGER-ID:14+GRP REFERENZ+++MES REFE
RENZ'
    USX+DAT001+5412345123450:14+5411234512300:14+GRP002+++MES003'
```

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

```
UST+1+5'
    UST+1+5'
```

```
UNT+10+AUT00001'
    UNT+10+AUT00001'
```

```
UNZ+1+12345555'
    UNZ+5+12345555'
```