EANCOM 2002 Syntax 4

Edition 2016_Update 2021

Security key and certficate management message (KEYMAN)

Einführung

Introduction

The following message specification is based on the publication of the "Security Key And Certficate Management Message" of GS1 Global in syntax 4.

Status

MESSAGE TYPE: KEYMAN
REFERENCE DIRECTORY: D.01B
EANCOM® SUBSET VERSION: 003

Definition

KEYMAN is a message providing for security key and certificate management. The message can be used to transmit a public key or a reference to a certificate used with asymmetric algorithms.

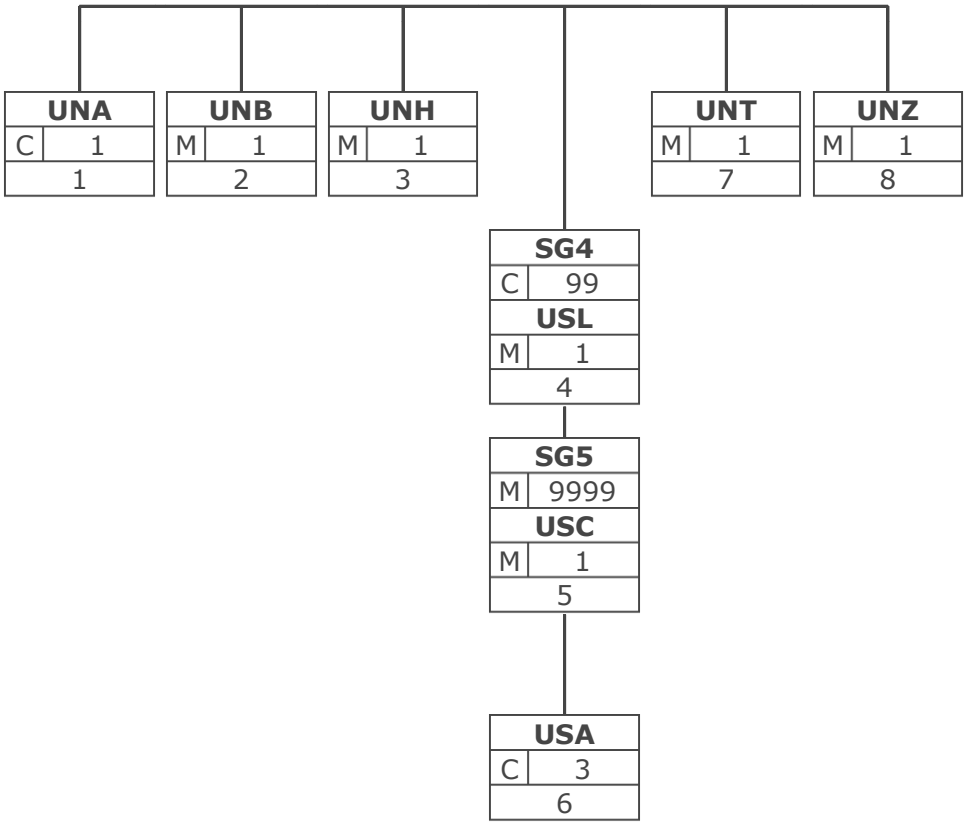
The security key and certificate management message (KEYMAN) may be used for both national and international trade. It is based on universal practice related to administration, commerce and transport, and is not dependent on the type of business or industry.

Principles

The message may be used to deliver security keys, certificates, or certification paths (this includes requesting other key and certificate management actions, for example renewing, replacing or revoking certificates, and delivering other information, such as certificate status), and it may be used to deliver lists of certificates (for e example to indicate which certificates have been revoked).

A security key and certificate management message can be used to deliver keys, certificates, and related information.

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
SG4		C	99	USL-SG5
USL	4	M	1	Security list status
SG5		M	9999	USC-USA
USC	5	M	1	Certificate
USA	6	C	3	Security algorithm
UNT	7	M	1	Message trailer
UNZ	8	M	1	Interchange trailer

Max. Occ. = Maximum occurrence of the segment/group, Status: M=Mandatory, C=Conditional, R=Required, O=Optional, A=Advised, D=Dependent

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'`

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.	
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	*	KEYMAN
	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 KEYMAN under the control of the United Nations.
Example:

Example: `UNH+KEY0001+KEYMAN:4:1:UN:EAN001:ABC'`
Example: `UNH+KEY0001+KEYMAN: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.	
	SG4	C	99	USL-SG5
	A group of segments containing lists of certificates or public keys. The group shall be used to group together certificates of similar status - i.e., which are still valid, or which may be invalid for some reason.			
4	**USL**	M	1	Security list status
	To specify the status of security objects, such as keys or certificates to be delivered in a list, and the corresponding list parameters.			

Business Term	DE	EDIFACT	Format	St	*	Description
	0567	Security status, coded	an..3	M	*	1 Valid 2 Revoked 6 Expired Identification of the security element (key or certificate, for instance) status.
	S504	List parameter		R		
	0575	List parameter qualifier	an..3	M	*	ZZZ Mutually defined
	0558	List parameter	an..70	M		Specification of the list requested or delivered.

A segment identifying valid, revoked, unknown or discontinued items. These items may be certificates (e.g., valid, revoked) or public keys (e.g., valid or discontinued).
There may be several different USL segments within this message, if the delivery implies more than one list of certificates or public keys. The different lists may be identified by the list parameters.
Example:
USL+1+ZZZ:ABC-LIST'

Example: `USL+1+ZZZ:ABC-LIST'`

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	C	99	USL-SG5	
	A group of segments containing lists of certificates or public keys. The group shall be used to group together certificates of similar status - i.e., which are still valid, or which may be invalid for some reason.				
	SG5	M	9999	USC-USA	
	A group of segments containing the data necessary to validate the security methods applied to the message/package, when asymmetric algorithms are used (as defined in Part 5 of ISO 9735). This group shall be used in the delivery of lists of keys or certificates of similar status.				
5	**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+X+3:X:X:2+3'`
Example: `USC+AXZ4711+4::5412345000006:2+3'`

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	C	99	USL-SG5	
	A group of segments containing lists of certificates or public keys. The group shall be used to group together certificates of similar status - i.e., which are still valid, or which may be invalid for some reason.				
	SG5	M	9999	USC-USA	
	A group of segments containing the data necessary to validate the security methods applied to the message/package, when asymmetric algorithms are used (as defined in Part 5 of ISO 9735). This group shall be used in the delivery of lists of keys or certificates of similar status.				
6	**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
	S503	Algorithm parameter		O		
	0531	Algorithm parameter qualifier	an..3	M	*	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.
	0554	Algorithm parameter value	an..51	M		Value of the exponent of the a public key.
	S503	Algorithm parameter		C		
	0531	Algorithm parameter qualifier	an..3	M	*	12 Modulus
	0554	Algorithm parameter value	an..51	M		Specification of the public key

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.
Please note that the DEG S503 is repeated twice according to EDIFACT syntax 4 rules, as repetition separator the asterisk (*) is used.
Example:

Example: `USA+6:16:1:10:1:7:1+13:X'`
Example: `USA+6:16:1:10:1:7:1+13:010001*12:CF8516555.....7E7406D7'`

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.	
7	**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+5+KEY0001'`
Example: `UNT+5+KEY0001'`

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 **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'`

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

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.

Used Codes

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.
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.
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.
0054	Message release number Release number within the current message version number.

Used Codes

1	First release Message approved and issued in the first release of the year 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.
KEYMAN	
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.
5	EDIFACT structure generation date and time Date and time of generation of the secured EDIFACT structure.

Used Codes

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.
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).
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.

Used Codes

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).
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).

Used Codes

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.
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.

Used Codes

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.

Used Codes

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.
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.
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).
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.
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.

Used Codes

4	Release character Specifies that this is the release character.
5	Repetition separator Specifies that this is the separator between repeating data elements.
0567	Security status, coded Identification of the security element (key or certificate, for instance) status.
1	Valid The security element is valid.
2	Revoked The security element has been revoked.
6	Expired The validity period of the security element is expired.
0575	List parameter qualifier Specification of the type of list parameter.
ZZZ	Mutually defined Mutually defined between trading partners.
0577	Security party qualifier Identification of the role of the security party.
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.
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+KEY0001+KEYMAN:4:1:UN:EAN001:ABC'
```
UNH+KEY0001+KEYMAN:4:1:UN:EAN001'

```
USL+1+ZZZ:ABC-LIST'
USC+X+3:X:X:2+3'
```
USC+AXZ4711+4::5412345000006:2+3'

```
USA+6:16:1:10:1:7:1+13:X'
```
USA+6:16:1:10:1:7:1+13:010001*12:CF8516555.....7E7406D7'

```
UNT+5+KEY0001'
```
UNT+5+KEY0001'

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