

EANCOM[®] 2002 S4

KEYMAN

Security key and certificate management message

Edition 2016

1. Introduction.....	2
2. Message Structure Chart	3
3. Branching Diagram.....	4
4. Segments Description	5
5. Segments Layout.....	6
6. Example(s)	16

1. Introduction

Status

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

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

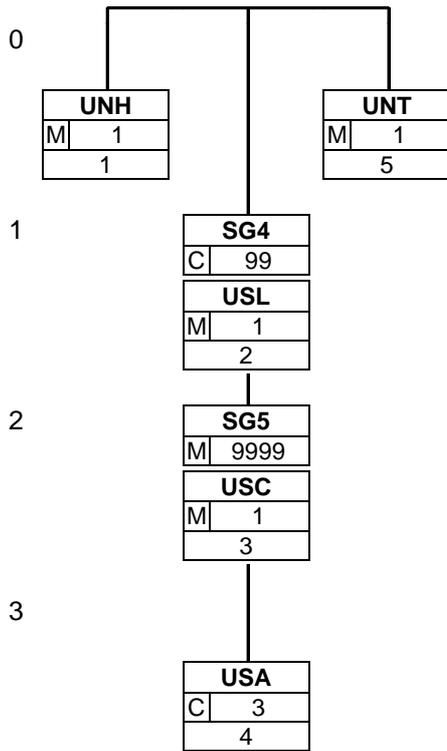
The message may be used to deliver security keys, certificates, or certification paths (this includes requesting other key and certificate management actions, for example renewing, replacing or revoking certificates, and delivering other information, such as certificate status), and it may be used to deliver lists of certificates (for example to indicate which certificates have been revoked).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

2. Message Structure Chart

UNH	1	M	1	- Message header
SG4		C	99	- USL-SG5
USL	2	M	1	- Security list status
SG5		M	9999	- USC-USA
USC	3	M	1	- Certificate
USA	4	C	3	- Security algorithm
UNT	5	M	1	- Message trailer

3. Branching Diagram



4. Segments Description

UNH - M 1	- Message header This segment is used to head, identify and specify a message.
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.
USL - M 1	- Security list status 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).
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.
USC - M 1	- Certificate This segment either contains information regarding the certificate, and identifies the certification authority which has generated the certificate, or is used to identify bilaterally interchanged signature keys.
USA - C 3	- Security algorithm This segment is used to identify a security algorithm, the technical usage made of it, and contains the technical parameters required in order to generate the digital signature.
UNT - M 1	- Message trailer A service segment ending a message, giving the total number of segments and the control reference number of the message.

5. Segments Layout

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

Notes:

1. The segments are presented in the sequence in which they appear in the message. The segment or segment group tag is followed by the (M)andatory / (C)onditional indicator, the maximum number of occurrences and the segment description.
2. Reading from left to right, in column one, the data element tags and descriptions are shown, followed by in the second column the EDIFACT status (M or C), the field format, and the picture of the data elements. These first pieces of information constitute the original EDIFACT segment layout.

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

- 2.1 (M)andatory data elements in EDIFACT segments retain their status in EANCOM®.
- 2.2 Additionally, there are five types of status for data elements with a (C)onditional EDIFACT status, whether for simple, component or composite data elements. These are listed below and can be identified when relevant by the following abbreviations:

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

- 2.3 If a composite is flagged as **N, NOT USED**, all data elements within that composite will have blank status indicators assigned to them.
3. Status indicators detailed in the fourth column which directly relate to the code values detailed in the fifth **column** may have two values:

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

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

5. Segments Layout

Segment number: 1

UNH - M 1 - Message header		EDIFACT	GS1	*	Description
Function: To head, identify and specify a message.					
Notes: 1. Data element S009/0057 is retained for upward compatibility. The use of S016 and/or S017 is encouraged in preference. 2. The combination of the values carried in data elements 0062 and S009 shall be used to identify uniquely the message within its group (if used) or if not used, within its interchange, for the purpose of acknowledgement.					
0062	Message reference number	M an..14	M		Sender's unique message reference. Sequence number of messages in the interchange. DE 0062 in UNT will have the same value. Generated by the sender.
S009	MESSAGE IDENTIFIER	M	M		
0065	Message type	M an..6	M	*	KEYMAN = Security key and certificate management message
0052	Message version number	M an..3	M	*	4 = Service message, version 4
0054	Message release number	M an..3	M	*	1 = First release
0051	Controlling agency, coded	M an..3	M	*	UN = UN/CEFACT
0057	Association assigned code	C an..6	R	*	EAN001 = GS1 version control number (GS1 Permanent Code)
0110	Code list directory version number	C an..6	O		This data element can be used to identify the codelist agreed by the interchange partners, e.g. EAN001 = EANCOM 2002 S4 codelist released on 01.12.2001 by GS1.
0113	Message type sub-function identification	C an..6	N		
0068	Common access reference	C an..35	N		
S010	STATUS OF THE TRANSFER	C	N		
0070	Sequence of transfers	M n..2			
0073	First and last transfer	C a1			
S016	MESSAGE SUBSET IDENTIFICATION	C	N		
0115	Message subset identification	M an..14			
0116	Message subset version number	C an..3			
0118	Message subset release number	C an..3			
0051	Controlling agency, coded	C an..3			
S017	MESSAGE IMPLEMENTATION GUIDELINE IDENTIFICATION	C	N		
0121	Message implementation guideline identification	M an..14			
0122	Message implementation guideline version number	C an..3			
0124	Message implementation	C an..3			

5. Segments Layout

Segment number: 1

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

Segment Notes:

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

DE's 0065, 0052, 0054, and 0051: Indicate that the message is an UNSM KEYMAN under the control of the United Nations.

Example:

UNH+KEY0001+KEYMAN:4:1:UN:EAN001'

5. Segments Layout

Segment number: 2

SG4	- C	99 - USL-SG5			
USL	- M	1 - Security list status			
Function:					
To specify the status of security objects, such as keys or certificates to be delivered in a list, and the corresponding list parameters.					
			EDIFACT	GS1	* Description
0567	Security status, coded		M an..3	M	* 1 = Valid 2 = Revoked 6 = Expired Identification of the security element (key or certificate, for instance) status.
S504	LIST PARAMETER		C	R	
0575	List parameter qualifier		M an..3	M	* ZZZ = Mutually defined
0558	List parameter		M an..70	M	Specification of the list requested or delivered.
Segment Notes:					
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'					

5. Segments Layout

Segment number: 3

SG4	- C	99 - USL-SG5
SG5	- M	9999 - USC-USA
USC	- M	1 - Certificate

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

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

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

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

5. Segments Layout

Segment number: 3

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

Segment Notes:

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

1. Use of USC for certificate reference:

A certificate reference (DE 0536) and trusted third party (DEG S500, DE 0577 = 4 and DEG S500, DE 511) can be identified.

Example 1:

USC+AXZ4711+4::5412345000006:2+3'

2. Use of USC for reference to signature keys:

Identification of the name of the signature key in DEG S500, DE 0538 (DEG S500, DE 0577 = 3).

The interchange of signature keys and the references have to be bilaterally agreed between the partners.

Example 2:

USC++3:PUBLIC KEY 01'

5. Segments Layout

Segment number: 4

SG4	- C	99 - USL-SG5
SG5	- M	9999 - USC-USA
USA	- C	3 - Security algorithm

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

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

	EDIFACT	GS1	*	Description
S502	SECURITY ALGORITHM	M	M	
0523	Use of algorithm, coded	Man..3	M	* 6 = Owner signing
0525	Cryptographic mode of operation, coded	C an..3	R	* 16 = DSMR Specification of the cryptographic mode of operation used for the algorithm. Note: The cryptographic mode of operation are the security functions authenticity, integrity and non-repudiation of origin. The digital signature includes all three security functions.
0533	Mode of operation code list identifier	C an..3	R	* 1 = UN/CEFACT
0527	Algorithm, coded	C an..3	R	10 = RSA 17 = ECC Identification of the algorithm in order to generate the digital signature. The algorithms above are recommended.
0529	Algorithm code list identifier	C an..3	R	* 1 = UN/CEFACT
0591	Padding mechanism, coded	C an..3	R	* 7 = ISO 9796 #2 padding Note: "ISO 9796 #2 padding" specifies the technical standard which is facilitating the security service "digital signature scheme giving message recovery" specified in DE 0525.
0601	Padding mechanism code list identifier	C an..3	R	* 1 = UN/CEFACT
S503	ALGORITHM PARAMETER	C	O	
0531	Algorithm parameter qualifier	Man..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	Man..512	M	Value of the exponent of the a public key.
S503	ALGORITHM PARAMETER	C	C	
0531	Algorithm parameter qualifier	Man..3	M	* 12 = Modulus
0554	Algorithm parameter value	Man..512	M	Specification of the public key

5. Segments Layout

Segment Notes:

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

5. Segments Layout

Segment number: 4

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

Example:

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

5. Segments Layout

Segment number: 5

UNT - M 1 - Message trailer					
Function: To end and check the completeness of a message.					
Notes: 1. 0062, the value shall be identical to the value in 0062 in the corresponding UNH segment.					
		EDIFACT	GS1	*	Description
0074	Number of segments in a message	M n..10	M		The total number of segments in the message is detailed here.
0062	Message reference number	M an..14	M		The message reference number detailed here should equal the one specified in the UNH segment.
Segment Notes: A service segment ending a message, giving the total number of segments and the control reference number of the message. Example: UNT+5+KEY0001'					

6. Examples

The following examples will show how the message type KEYMAN can be used in order to transmit either a public key or a certificate reference.

Example 1

In the following example the public key of the sender identified with the GLN 4012345262698 is sent to a business partner in order to enable him to verify digital signatures in future transmissions.

UNH+KEY0001+KEYMAN:4:1:UN:EAN001'	Message header of the service message KEYMAN
USL+1+ZZZ:ABC-LIST'	The list of valid keys is identified as ABC-LIST.
USC++3:PUBLIC KEY 01'	The transmitted public key is identified as PUBLIC KEY 01
USA+6:16:1:10:1:7:1+13:010001*12:CF8516555....7E7406D7'	The algorithm used for generating digital signatures is RSA, the padding mechanism is specified in ISO 9796 # 2. The modulus of the public key is 010001. The public key of the sender is CF8516555.....7E7406D7.
UNT+5+KEY0001'	Message trailer, the total number of segments equals 5

Example 2

In the following example a reference to a certificate issued by a trust centre identified with the GLN 5412345000006 is sent to a business partner in order to enable him to verify digital signatures in future transmissions.

UNH+KEY0001+KEYMAN:4:1:UN:EAN001'	Message header of the service message KEYMAN
USL+1+ZZZ:ABC-LIST'	The list of valid certificates is identified as ABC-LIST.
USC+AXZ4711+4::5412345000006:2+3'	The reference of the certificate issued by the trust centre identified with the GLN 5412345000006 is AXZ4711. The syntax of the certificate is X.509.
USA+6:16:1:10:1:7:1'	The algorithm used for generating digital signatures is RSA, the padding mechanism is specified in ISO 9796 # 2.
UNT+5+KEY0001'	Message trailer, the total number of segments equals 5

Note:

The EDI interchange will include the UNB..UNZ segments and, if applicable, the UNG..UNE segments. (See part 1 section 5.7)