SWG-F D6
MESSAGE IMPLEMENTATION GUIDELINE
OF THE UN/EDIFACT
SECURE AUTHENTICATION & ACKNOWLEDGEMENT
MESSAGE

AUTACK

DRAFT 0.6m

This simplified Message Implementation Guide is designed to accommodate the separate services of authentication and acknowledgement for which AUTACK can be used, as described in the EDIFACT Finance Group's Recommended Message Flow Guidelines.

The security part of the recommendation guidelines identify specific crypto techniques to be used.

It provides an interim security solution for syntax 3 message implementations, facilitating a future migration to syntax version 4.

Draft: **0.6m**
Prepared by: **SWG-F D6**
Version: **Syntax 3/4**
Date: **April 1999**

SPECIFICATION OF THE SECURE AUTHENTICATION & ACKNOWLEDGEMENT MESSAGE

AUTACK

Contents

This message implementation guide for AUTACK is based on the latest edition of the ISO 9735 Syntax 4 version, but this has been ‘adapted’ to conform to EDIFACT syntax 3 whilst still retaining the functionality of the latest AUTACK. This step is essential in order to meet the business requirements of effectively securing messages conforming to syntax 3.

Brief Explanation of Content

This page briefly describes the chapters and sections of the document, and suggests how readers with different needs and interests can approach the document.

Chapter 1 The introduction and scope outlines the usage of AUTACK that this document defines, that is, the authentication and acknowledgement requirements described in the Recommended Message Flow Guidelines.

There are two ways in which the reader can approach the further chapters of this Message Implementation Guide.

The business-oriented reader can continue reading through Chapter 2 onwards, as this takes the reader from a business level view, identifying the pieces of information required and pointing to where each piece goes in the message.

The programmer-reader can go to Chapter 5 where the message is presented in an overview form which points to where, in Chapter 4, each part of the message is described in detail

Chapter 2 Section 1 The purpose of this overview is to give a picture of the structure of the interchange, the transaction messages and the authentication message, and to show how the parts of the authentication message relate to the parts of the interchange.

Section 3 This describes in business terms the blocks of information that are needed in order to carry out a securing function on an interchange. For the contents of the other messages in the interchange that is secured, see the appropriate Message Implementation Guide.

Section 4 This overview shows the segments and segment groups of the full AUTACK message and relates them to the logical structure of the message which the previous section 2.1 portrays.

Chapter 3 This takes each piece of business information identified in section 2.3 and points to the precise place within the AUTACK message where each piece of information fits. There are two separate information content indices, one for the authentication scenario, the other for the acknowledgement scenario.

Chapter 4 This describes each segment of the message and how it is used. The description consists of a detailed table, and then further explanatory text and an example. There are pointers for each of the pieces of information identified in section 2.3 and chapter 3.

At the beginning of the chapter, there is an annotated dummy table that explains the information contained within the table.

Chapter 5 Section 1 This overview shows the segments and segment groups of the full AUTACK message.

Section 2 This gives the same information for the full message as it appears in the previous section 5.1 but presented in a graphical form.

1. INTRODUCTION & SCOPE

The Secure Authentication and Acknowledgement message AUTACK is used, as defined within this document, for the two purposes specified in the Recommended Message Flow guidelines. These are:-

- authentication of an interchange being sent
- ensuring integrity of content by hashing and signing the entire set of transaction messages in the interchange
- ensuring origin authentication and non-repudiation of origin by the sender's digital signature of the sent interchange
- acknowledgement of a received interchange
- ensuring non-repudiation of receipt by the recipient's digital signature of the hashed content of the received interchange

The applied security procedures shall be agreed to by trading partners and specified in an interchange agreement.

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 the relevant data such as the reference to the cryptographic methods used, the reference numbers and the date and time of the original EDIFACT structures.

1.1 AUTACK For Authentication

AUTACK, used as an authentication message, is sent by the originator of an interchange consisting of one or more EDIFACT transaction messages, or by a party having authority to act on behalf of the originator, to give:-

- origin authentication,
- validation of sequence integrity (assuming a system of sequentially numbering messages is used and is covered by authentication.)
- non-repudiation of origin

The authentication is implemented in the following steps:

- calculation of the hashed value of the interchange
- the hash value is then used as input to calculate the digital signature, i.e. it is encrypted under the originator's private key
- the digital signature is put into the AUTACK
- if necessary, a second authentication can be made by another signatory. The hash value is calculated again (to allow detection of changes to the data between signatures) and the signature may be computed using a second private key and put into the AUTACK to provide a double key.

The recipient will check that the received interchange matches the hash value extracted from the sender's digital signature, and this verifies both the validity of the content and of the origin..

If the sender wishes to take advantage of the non-repudiation of receipt coming back from the recipient in the acknowledgement AUTACK, the original computed hash value must be retained for comparison with the secure acknowledgement**.**

1.2 Confirmation/Acknowledgement

Authentication gives the recipient of an interchange confidence in the veracity of the interchange. The response, either acceptance, or rejection on syntax grounds, is given by the CONTRL message. It too needs to be covered by an authentication AUTACK.

However, this response interchange only gives a confirmation of receipt. If the original interchange is being accepted for further processing, it is important to provide evidence of the content that was received.
This is achieved by adding a second AUTACK into the response interchange, which is an acknowledgment AUTACK as described in the next sub-section.

So a rejection response interchange would consist of:-

- a CONTRL receipt message
- an AUTACK that authenticates the CONTRL message.

And an acceptance response interchange would consist of:-

- a CONTRL receipt message
- an AUTACK that authenticates the CONTRL message.
- an AUTACK that acknowledges the received content of the original interchange

Whether or not the sender of the original interchange takes full advantage of the 'non-repudiation of receipt' which the acknowledgement AUTACK provides is a decision for the original sender. What they will need to do is described in the next sub-section.

1.3 AUTACK for Acknowledgement

AUTACK, used as an acknowledgement message, is sent by the recipient of the received secured EDIFACT interchange, or by a party having authority to act on behalf of the recipient, to give:-

- non-repudiation of receipt of the interchange

The acknowledgement is implemented in the following steps:

- the original hashed value of the interchange is derived from the received digital signature
- the hash value is then used to calculate the recipient's digital signature, as described previously
- the recipient's digital signature is put into the AUTACK

If the sender of the original interchange wishes to take advantage of the non-repudiation of receipt given by the acknowledgement AUTACK, they will have retained the original computed hash value which they can then compare with the hash value as perceived by the recipient. It is extracted from the recipient's digital signature. This comparison gives

- validation of integrity of content
- validation of completeness

1.4 General Note

Secure acknowledgement is only meaningful for an authentication AUTACK and its referenced interchange.

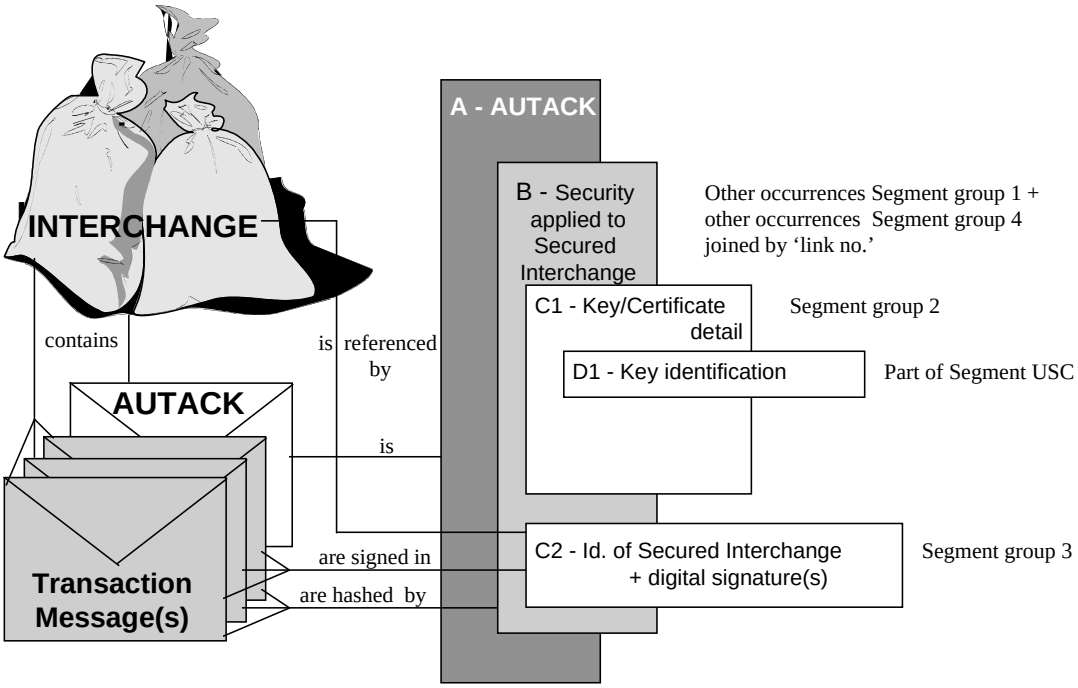
To prevent endless loops, an acknowledgement AUTACK shall ***not*** require its recipient to send back an AUTACK acknowledgement message.

2. STRUCTURE OVERVIEW

2.1 Overview

The purpose of this overview is to give a picture of the structure of the interchange, the transaction messages and the authentication message, and to show how the parts of the authentication message relate to the parts of the interchange.

The AUTACK message, as described here for simplified use in the context of the recommended message flow, secures one set of information; all of the transaction messages within a referenced interchange, from the first UNH to the last UNT. The AUTACK is added at the end of the interchange, after the transaction messages.



The Authentication and Acknowledgement message AUTACK consists of several nested levels of information, but not all are used in the simplified implementation described in this document.

A covers the whole AUTACK message and includes information that relates to the whole message, such as the sender and receiver

B specifies the security function and mechanisms that have been applied to the interchange. (This level can occur a second time to allow for double signatures.)

C1 identifies the key or certificate details that relate to the set of information that is encompassed by the B-level in which it occurs.

D1 identifies the key used from the 'key agreement' exchanged previously. The full message would allow the certificate to be fully detailed here if it had not been previously exchanged.

C2 specifies the identity of the referenced interchange to which the B-level 'set' relates. There can be two sets in this simplified MIG, allowing a double signature on one referenced interchange.

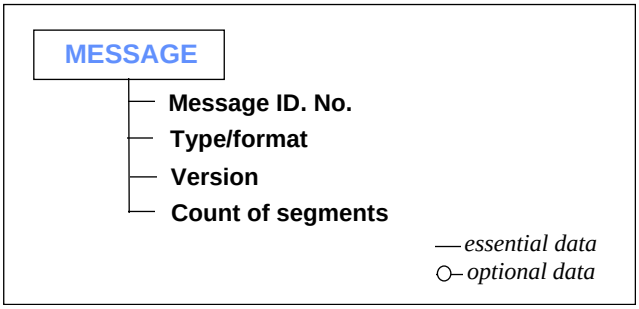
2.2 Interchange and Message Infrastructure Information

The interchange ‘sack’ which contains the transaction messages, and the AUTACK message, need an identity or ‘label’.

The Message Implementation Guides for the messages that the AUTACK is used to authenticate will describe the interchange ‘label’, and should be referred to as necessary.

The figure below shows the pieces of information for the message ‘envelope label’ for the AUTACK.

This also comprises two segments, a message header segment (UNH) and a message trailer segment (UNT). The message identity no. appears in both the header and trailer, so that the end-to-end integrity of the message can be checked. The count of segments enables a further check to be made. The message type/format and version tells the receiving software exactly what layout the message data conforms to. In this case, the message type/format. is AUTACK and it conforms to version 3 of the EDIFACT message syntax.



There must be only one message header (UNH) and message trailer (UNT) for each message. However, there can be several messages in an interchange; each UNH-?-UNT set is a message. The information identified in the diagrams is conveyed within the segments as follows:-

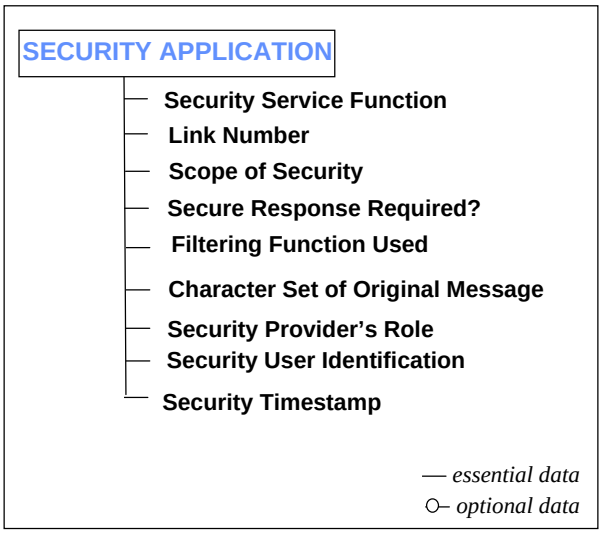
Name of Information	*in Chapter/Section*	*UN/EDIFACT Segment/Element*	
Message Type/Format	4.1	UNH	S009/0065
Message Version	4.1	UNH	S009/0052-4
Message ID No.	4.1	UNH	0062
and in	4.12	UNT	0062
Message Count of Segments	4.12	UNT	0074

Note that the Message ID No. is normally a serial number of the messages within the interchange, starting from 1. For example, if there are four payment messages and an accompanying AUTACK, this will be 5 for the AUTACK.

2.3 Information Blocks

This sub-section describes in business terms the blocks of information that are needed in order to carry out a securing function on an interchange. For the contents of the messages in the interchange that is secured, see the appropriate Message Implementation Guide.

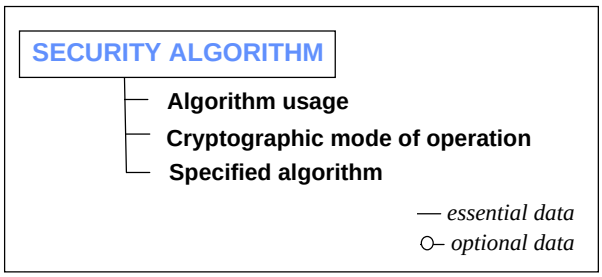
In the securing function described here, which is in the context of the recommended message flow, there is only one set of information secured. That set encompasses all of the transaction messages within a single referenced interchange, from the first UNH to the last UNT.



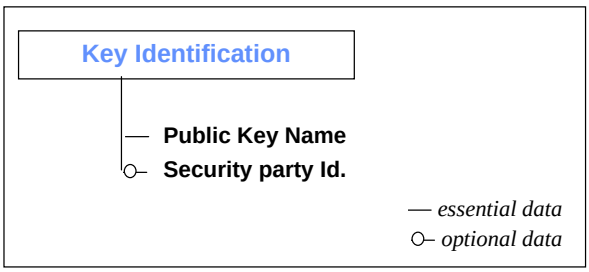
These security details specify the function and scope of security as applied to the interchange. In this simplified MIG the scope is from and including the first UNH to the last UNT which precedes where the AUTACK will be placed.
The original character set of the interchange may be stated. The security user can be identified and their role stated. A timestamp is also given.

The link number connects this security detail with the referenced interchange. See the note at the end of this section.

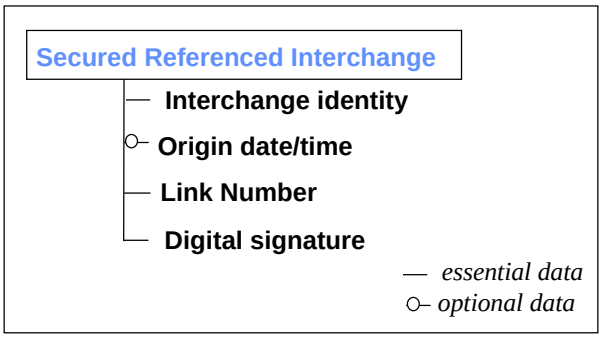
Associated with the block of information about security applied to the Interchange, there are also details about the algorithm used. These indicate the use that is made of the algorithm specified, and the way in which it is used.



In addition, there are further 'lower level' blocks of information, as follow.



Key sets will have been previously exchanged. The keys used only need to be identified by reference to their identity. Identification may also need the id of the issuing security party to be specified in order to be unique.



This block of information identifies the interchange that is to be secured according to the securing details given. The origin date/time of the referenced interchange may also be stated.

The digital signature of the hashed value of the Interchange is also given.

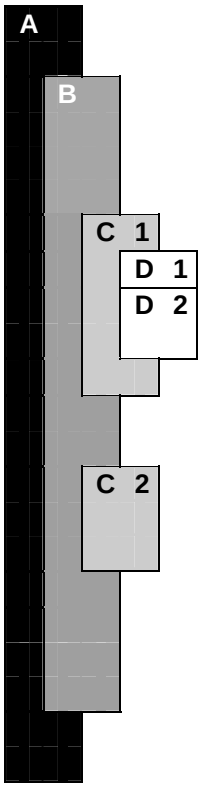
The link number connects the securing details with the referenced interchange. The full message design allows for multiple entities to be referenced and secured, potentially using different securing techniques. The link number identifies each different ‘set’ which techniques apply to which referenced entities. This link number is essential even though the simplified usage described here only references one interchange. It is a necessity of message design rather than business information.

When there is a second signature, there is a second complete 'set' in the message even though it refers to the same entity. The link number for the second set is 2.

2.4 Usage of AUTACK

This overview shows the segments and segment groups of the full AUTACK message and relates them to the logical structure of the message which the previous section 2.1 portrays. It is then followed by Chapter 3 which takes each piece of business information identified in section 2.3 and points to the precise place within AUTACK where each piece of information fits.

In the simplified usage that this document describes, some parts of the AUTACK message are not used. The 'M/C' columns indicate whether or not the segment or group is necessary, M indicating it is mandatory and C that it is conditional in the full message. The R indicates that it is needed, and N that it is not used, in this simplified usage. The first 'occurs' columns indicates the number of times a segment or segment group can occur in the full message, while the second shows that this is limited within the simplified usage described in Chapter 4. The 'see 4.n' column indicates the section in Chapter 4 where the segment is described.



Tag	*Data Segment Name*	*M/C (1)*	*(2)*	*Occurs (1)*	*(2)*	*See 4.n*
UNH	Message Header	M		1		4.1
	Segment Group 1	M		99	2	
USH	Security Header	M		1		4.2
USA	Security Algorithm	C	R	3	1	4.3
	Segment Group 2	C	C	2	1	
USC	Certificate	M		1		4.4
USA	*Security Algorithm*	*C*	*N*	*3*	*0*	*4.5*
USR	*Security Result*	*C*	*N*	*1*	*0*	*4.6*
USB	Secured Data Identification	M		1		4.7
	Segment Group 3	M		9999	1	
USX	Security References	M		1		4.8
USY	Security on References	M		9	2	4.9
	Segment Group 4	M		99	2	
UST	Security Trailer	M		1		4.10
USR	*Security Result*	*C*	*N*	*1*	*0*	*4.11*
UNT	Message Trailer	M		1		4.12

Note that there is no structural link connecting the security header (segment group 1), the security trailer (segment group 4), the item being secured and the digital signature (segment group 3). A 'link number' is used for each separately secured 'set' of information, i.e. all the instances of segment groups 1-4 that relate together and the referenced EDIFACT entities but a link is made logically by the data content of the 'link number'.

In general terms, the message is used in the following simplified way:-

2.4.1 For Authentication

The authentication AUTACK uses one occurrence of the USX 'Security References' segment to reference the interchange that it authenticates. With the USX segment there shall be one corresponding USY 'Security on References' segment and this contains the security result, i.e. the digital signature computed on the hash value of the referenced interchange.

Details about the security functions performed shall be contained in the AUTACK security header group, i.e. ‘B’ in the diagram. One occurrence of the USA segment following the USH is used to indicate the hash algorithm used. The USC segment is used to refer to the pre-arranged set of keys that are being used. It is not necessary to specify which digital signature algorithm used, or the specific parameters, as these are detailed on the Public Key Document. (For information, the algorithm recommended is RSA with ISO 9796 - Part 1 padding, 65537 as the public exponent and modulus length of 1024.)

The USY and USH segments for the referenced EDIFACT structure shall be linked using the ‘link reference’ which is in both segments. One occurrence of the USH, USY and UST groups is used for a single signature and the link number must be 1. Two occurrences are used for double signature, and the link number is 1 for the first set and 2 for the second. .

As defined in EDIFACT security documentation ISO9735 Part 6, the AUTACK itself does not need to be secured because it conveys a digital signature.

2.4.2 For Acknowledgement

The acknowledgement AUTACK uses one occurrence of the USX 'Security References' segment to reference the original interchange that it is acknowledging. With the USX segment there shall be one corresponding USY 'Security on References' segment which contains the security result, i.e. the digital signature of the recipient of the original interchange computed on the hash value of the original interchange.

Details about the security functions performed shall be contained in the AUTACK security header group, i.e. ‘B’ in the diagram. The USC segment is used to refer to the pre-arranged set of keys that are being used by the acknowledgement sender.

The USY and USH segments for the referenced EDIFACT structure shall be linked using the ‘link reference’ which is in both segments. Although this is logically unnecessary, given only one occurrence of USH and USY is used, the design of the message insists on it being present.

As defined in EDIFACT security documentation ISO9735 Part 6, the AUTACK itself does not need to be secured because it conveys a digital signature.

3 INFORMATION CONTENT

There are two separate information content indices, each for a particular usage scenario.

3.1 Authentication Scenario

The essential 'business' pieces of information, required when the message is used in its authentication role to secure an interchange, are conveyed within the UN/EDIFACT message AUTACK as follows:-

Name of Information	*Chapter/Section*	*UN/EDIFACT Segment/Element*	
Security on Secured Interchange			
Security service function	4.2	USH	0501
Non-repudiation of origin			
Link number	4.2	USH	0534
Scope of security	4.2	USH	0541
First UNH to Last UNT of transaction messages			
No acknowledgement required	4.2	USH	0503
Filtering function used	4.2	USH	0505
Hexadecimal			
EDC			
Character set of original message	4.2	USH	0507
ASCII 7 bit			
ASCII 8 bit			
Security provider role	4.2	USH	0509
Issuer			
Security time stamp	4.2	USH	S501/0338 & 0314
Security Algorithm			
Algorithm usage	4.3	USA	S502/0523
Owner hashing			
Specified algorithm	4.3	USA	S502/0527
SHA-1			
Certificate Key/Identififcation			
Public key name	4.4	USC	0538
Security party id.	4.4	USC	0511
Referenced entity			
Interchange identity	4.8	USX	0020
Origin of interchange date/time	4.8	USX	S501/0338
Link number	4.9	USY	0534
Filtered Digital signature on original interchange	4.9	USY	S508/0560
AUTACK Message Data			
No acknowledgement required	4.7	USB	0503
Generation date/time	4.7	USB	S501/0338
Interchange sender id.	4.7	USB	S002/0004
Interchange receiver id.	4.7	USB	S003/0010

3.2 Acknowledgement Scenario

The essential 'business' pieces of information, required when the message is used in its acknowledgement role to securely acknowledge an interchange, are conveyed within the UN/EDIFACT message AUTACK as follows:-

Name of Information	*Chapter/Section*	*UN/EDIFACT Segment/Element*	
Security Application			
Security service function	4.2	USH	0501
Non-repudiation of receipt			
Link number	4.2	USH	0534
Scope of security	4.2	USH	0541
First UNH to Last UNT of transaction messages			
No acknowledgement required	4.2	USH	0503
Filtering function used	4.2	USH	0505
Hexadecimal			
EDC			
Character set of original message	4.2	USH	0507
ASCII 7 bit			
ASCII 8 bit			
Security provider role	4.2	USH	0509
Issuer			
Security time stamp	4.2	USH	S501/0338 & 0314
Reference to Key/Certificate			
Public key name	4.4	USC	0538
Security party id.	4.4	USC	0511
Referenced entity			
Interchange identity	4.8	USX	0020
Origin date/time	4.8	USX	S501/0338
Link number	4.9	USY	0534
Filtered Digital signature on original hash	4.9	USY	S508/0560
AUTACK Message Data			
No acknowledgement required	4.7	USB	0503
Generation date/time	4.7	USB	S501/0338
Interchange sender id.	4.7	USB	S002/0004
Interchange receiver id.	4.7	USB	S003/0010

4 SEGMENT SPECIFICATION

This section describes each segment of the message and how it is used. The description consists of a detailed table, and then further explanatory text and an example. The table that follows is a dummy complete with annotations to explain the information contained in the table.

Column 1		2	3	4	5	6	7	8	
		Tag #	**Description of Data Field**	**M/C**	*****	**Format**		**Code**	Note
						UNB	+		9
		S001	SYNTAX IDENTIFIER	M	1				10
Interchange Syntax	⇨	0001	Syntax identifier	M		a4	:	UNOA	11
		0002	Syntax version number	M		n1	+	3	
Interchange ID No.	⇨	0020	INTERCHANGE CONTROL REFERENCE	M	1	an..14	+		12
		S005	*RECIPIENTS REFERENCE PASSWORD*	*N*	*1*				13
		0022	*Recipient's reference/password*			*an..14*	:		
		0032	*COMMUNICATIONS AGREEMENT ID*	*N*	*1*	*an..35*	+		
		0035	*TEST INDICATOR*	*N*	*1*	*n1*	'		14
							15		

Column 1 Identifies the business information and points to its place in the segment. This is then described in the text

Column 2 gives the UN/EDIFACT 'tag' which identifies the element. The tag comprises a letter and three digits for composite elements, or four digits for a single element. The single element equates to a 'field' in other data terminologies.

Column 3 gives the name of the element or data field.

Column 4 indicates whether the field is:-

- M = Mandatory, i.e. the field is defined as 'must be used' within the UN/EDIFACT design.
- R= Required, i.e. the field is defined as necessary within this message implementation guide, although it is defined as 'conditional' within the basic UN/EDIFACT design.
- D= Dependent, i.e. the field has, within this message implementation guide, dependency notes which describe the circumstance in which it is used, usually in relation to other fields. These fields are defined as 'conditional' within the basic UN/EDIFACT design.
- C = Conditional, i.e. the field is defined as 'conditional', both within this MIG and within the basic UN/EDIFACT design.
- N = Not used, i.e. no business requirement for the field has been identified within the message implementation guide. Such fields are conditional within the basic UN/EDIFACT design.

Column 5 indicates the number of possible occurrences of the element within this place in the segment.

Column 6 indicates the format and length of the field

a = alphabetic
n = numeric
an = alphanumeric
.. = variable length up to the number
absence of .. = fixed length of the number

At the head of this column, the segment tag is repeated. If you read this column and the one to the right which shows the punctuation, working down the rows you can easily build up what the segment actually looks like when communicated. Note 15 explains what to do if any particular element is not needed.

Column 7 shows the separator which normally follows the data field. See **note 15** for a detailed explanation about omitting conditional data.

Column 8 shows code value(s) which must be used in the field. These are explained in the text.
Note 9 the segment identifying 3-character 'tag' is part of the segment.
Note 10 this is the name of a composite set of data fields, as indicated by the letter and three digit tag. It identifies a set of data fields.
Note 11 this is a data field within the set, for which a code value exists.
Note 12 this is a data field which is not part of a composite set, i.e. it is a stand alone data element.
Note 13 fields which are not used are shown in italics.
(see also **Note 15** which explains how omitted elements are shown.)
Note 14 The terminator mark **'** of the last data field/element **must** always be used to indicate the end of the segment.
Note 15 Column 7 shows the separator which normally follows the data field. This may however change when some or all of the subsequent conditional data fields are omitted. The following example is used to illustrate the different situations which may arise.

	Tag#	Description	M/C	Format		Code
				BGM	+	
Field A	C002	DOCUMENT/MESSAGE NAME	C			
B	1001	Document/message name, coded	C	an..3	:	
C	1131	Code list qualifier	C	an..3	:	
D	3055	Code list responsible agency, coded	C	an..3	:	
E	1000	Document/message name	C	an..35	+	
F	1004	DOCUMENT/MESSAGE NUMBER	C	an..35	+	
G	1225	MESSAGE FUNCTION, CODED	C	an..3	+	
H	4343	RESPONSE TYPE, CODED	C	an..3	'	

If C and D fields within composite A are omitted, their separators are retained, or else E cannot be seen in its correct context. The segment would appear as follows:-

BGM+B:::E+F+G+H'

If C, D and E are all omitted, their separators are not retained as B becomes the last element used within the composite A. The segment appears as follows:-

BGM+B+F+G+H'

If 'stand-alone' elements F and G are also omitted, their separators are retained, or else H cannot be seen in its correct context. The segment appears as follows:-

BGM+B+++H'

However if H is also omitted, B is now the last element within the segment and it has the segment end separator. The segment appears as follows:-

BGM+B'

If, in this last example, the field E within composite A had been needed, the segment would have appeared as:-

BGM+B:::E'

4.1 UNH, MESSAGE HEADER (Mandatory, Occurs 1)

4.1.1 This segment specifies the beginning of each individual message, identifies the message within a range of messages sent, and specifies the message type version and release number used in formatting the information.

		Tag #	*Description*	*M/C*	*	*Format*		*Code*
						UNH	+	
Message reference Number	⇨	0062	MESSAGE REFERENCE NUMBER	M		an..14	+	
		S009	MESSAGE IDENTIFIER	M				
Message format	⇨	0065	Message type identifier	M		an..6	:	AUTACK
Message format Version	⇨	0052	Message type version number	M		an..3	:	3
	⇩	0054	Message type release number	M		an..3	:	1
See note 1	⇨	0051	Controlling agency	M		an..2	:	UN
See note 2	⇨	0057	Association assigned code	R		an..6	+	SECAUT SECACK
		0068	*COMMON ACCESS REFERENCE*	*N*		*an..35*	+	
		S010	*STATUS OF TRANSFER*	*N*				
		0070	*Sequence message transfer number*			*n..2*	:	
		0073	*First/last sequence message transfer Indication*			*a1*	'	

4.1.2 RULES

4.1.3 DATA REQUIREMENT

4.1.3.1 Message Reference Number (0062)

This contains a reference that is unique to the message, within a range of messages sent, and which is assigned by the sender incrementing sequentially from 1 for each message in the interchange. The same number must be entered in the UNT segment (Message Trailer) at the end of the message.

4.1.3.2 Message Format (0065)

This identifies the EDIFACT message type. For this message it must contain the code AUTACK, i.e. Secure authentication and acknowledgement message.

4.1.3.3 Message Format Version (0052)

This identifies the version of the syntax, in this case version 3, and the release number of the message.

Note 1 **- Controlling Agency (0051)**

This mandatory element **must** contain the code UN.

Note 2 - **Association Assigned Code (0057)**
This required element is used within the message to identify the implementation guidelines which describe how the message is used, in order for the recipient to interpret the message exactly. It should contain one of the following codes:-

Code	*Name*	*Description*
SECAUT	AUTACK in its authentication role	SEC identifies the Security Task Force (STF) of EDIFACT Finance Sub-Working Group (D6) as the body responsible for this documentation of the AUTACK message, and AUT identifies that the message is used in its authentication context.
SECACK	AUTACK in its acknowledgement role	SEC identifies the STF of D6 as the body responsible for this documentation of the AUTACK message used in its acknowledgement context.

4.1.4 EXAMPLE

UNH+1+AUTACK:3:1:UN:SECAUT'

Component	**Meaning**	**Description**
1	Message Reference Number	1st message in a series
AUTACK	Message Type Identifier	Secure authentication and acknowledgement message
3:1	Message Type Version and Release Number	Version 3, Release 1 of the UN/EDIFACT syntax (AUTACK is a syntax message)
UN	Controlling Agency	The UN is responsible for maintenance of the AUTACK message.
SECAUT	Association Assigned Code	D6 STF is responsible for the message specification and it is being used in the authentication role.

4.2 to 4.6 Segment Group 1 (Mandatory, Occurs 99, Limited to 2)

Tag	*Segment Name*	*M/C*		*Occurs*	
		(1)	*(2)*	*(1)*	*(2)*
USH	Security Header	M		1	
USA	Security Algorithm	C	R	1	

Segment group 2 (Conditional, 2)			C		1
USC	Certificate	M		1	
USA	Security Algorithm	C	N	3	0
USR	Security Result	C	N	1	0

Note: (1) indicates the full message specification,
(2) notes any change for this implementation

This segment group identifies the security service, scope, and security mechanisms applied, and includes the data necessary to carry out the validation calculations. It specifies the security service and algorithm(s) applied to the referenced entity.

The security service specifies the security function applied:-

- in the Authentication role, to the referenced entity:-
  - referenced entity non-repudiation of origin

  which implies (see ISO9735, Part 5)
  - referenced entity integrity
  - referenced entity origin authentication
- in the Acknowledgement role, to the original referenced entity:-
  - referenced entity non-repudiation of receipt

This documentation describes use of the AUTACK according to the simplified requirements of the Finance Sub-working Group. Here, the application of security is to the whole set of transaction messages within the interchange, i.e. from the first UNH to the last UNT of the interchange, but excluding the AUTACK. The authentication AUTACK follows the last transaction message and is immediately before the interchange trailer.
The CONTRL message is a transaction message as it is used to confirm receipt of, or to reject, business transactions. It is followed by an authentication AUTACK and this may in turn be followed by an acknowledgement AUTACK.

Each instance of this segment group needs to be associated with a security trailer group (segment group 4) and associated also with USY segment(s) in instances of segment group 3. Details in these parts of the message are logically related, and the association is made by a ‘link number’. This has the value 1 for the first set, which relate to a single signature or the first of two signatures. The link number is 2 for the set relating to the second signature.

The algorithm identified in the USA segment that follows the security header USH is the algorithm directly applied to the message content. It is a hash function, the result of which is used to compute the digital signature.

For non-repudiation of origin by means of a digital signature, the key(s) that are used will be identified by an identifying reference known to the receiving party in the USC of segment group 2.

4.2 USH, SECURITY HEADER (Mandatory, Occurs 1)

4.2.1 This segment specifies a security service function that is applied to the entity referenced in the USX of segment group 3.

		Tag #	*Description*	*M/C*	*	*Format*		*Code*
						USH	+	
Security service function	⇨	0501	SECURITY SERVICE, CODED	M	1	an..3	+	
Link number	⇨	0534	SECURITY REFERENCE NUMBER	M	1	an..14	+	
Scope of security	⇨	0541	SCOPE OF SECURITY APPLICATION, CODED	R	1	an..3	+	
Secure response required	⇨	0503	RESPONSE TYPE, CODED	R	1	an..3	+	
Filtering function used	⇨	0505	FILTER FUNCTION, CODED	R	1	an..3	+	
Character set of original Message	⇨	0507	ORIGINAL CHARACTER SET ENCODING, CODED	R	1	an..3	+	
Security provider role		0509	ROLE OF SECURITY PROVIDER, CODED	R	1	an..3	+	
		S500	SECURITY IDENTIFICATION DETAILS	D	1			
See note 1	⇨	0577	Security party qualifier	M		an..3	:	
		0538	*Key name*	*N*		*an..35*	:	
Security User Id.	⇨	0511	Security party id. Identification	R		an..17	:	
See note 2	⇨	0513	Security party Code list qualifier	C		an..3	:	
	⇩	0515	Security party Code list responsible Agency, coded	C		an..3	:	
		0586	*Security party name*	*N*		*an..35*	:	
		0586	*Security party name*	*N*		*an..35*	:	
		0586	*Security party name*	*N*		*an..35*	+	
		S500	SECURITY IDENTIFICATION DETAILS	D	1			
See note 1	⇨	0577	Security party qualifier	M		an..3	:	
		0538	*Key name*	*N*		*an..35*	:	
Security User Id.	⇨	0511	Security party id. Identification	R		an..17	:	
See note 2	⇨	0513	Security party code list qualifier	C		an..3	:	
	⇩	0515	Security party code list responsible Agency, coded	C		an..3	:	
		0586	*Security party name*	*N*		*an..35*	:	
		0586	*Security party name*	*N*		*an..35*	:	
		0586	*Security party name*	*N*		*an..35*	+	
		0520	*SECURITY SEQUENCE NUMBER*	*N*	*1*	*an..35*	+	
		S501	SECURITY DATE AND TIME	R	1			
See note 3	⇨	0517	Date and time qualifier	M		an..3	:	
Security time stamp	⇨	0338	Event date	R		n..8	:	
	⇩	0314	Event time	R		an..15		
		0336	*Time offset*	*N*		*n4*	'	

4.2.2 RULES

Security party identification in this segment should only be used if the parties involved in security are not unambiguously identified elsewhere

4.2.3 DATA REQUIREMENT

4.2.3.1 Security service function (0501)

This specifies the security function that is applied. Different security functions apply to different circumstances.

When the segment and segment group is being used in an authentication role, the following security function code is used:

Code	*Meaning*	*Description*
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.

When the segment and segment group is being used in an acknowledgement role, the following security function code is used:

Code	*Meaning*	*Description*
5	Non-repudiation of receipt	Non-repudiation of receipt protects the sender of an object message from the receiver's denial of having received the message.

4.2.3.2 Link number (0534)

This reference number links a particular USH segment with its corresponding UST segment, the value used is arbitrarily assigned but, within one message, the same value must not be used more than once.

4.2.3.3 Scope of security (0541)

This specifies the scope of application of the security service defined in the present header, i.e. it defines the data that have to be taken into account by the related cryptographic process. The following code must be used:-

Code	*Meaning*	*Description*
F01	First UNH to last UNT	From the first character of the UNH of the first transaction message to the last character of the UNT of the last transaction message in the referenced interchange.
ZZZ	Mutually agreed	The scope of the security application is defined in an agreement between sender and receiver.

4.2.3.4 Response required (0503)

This specifies whether a secure acknowledgement from the message recipient is required or not. If it is required, the message sender expects an AUTACK message to be sent back by the current message recipient to the current message sender, containing this acknowledgement**.** One of the following codes must be used:-

Code	*Meaning*	*Description*
1	No acknowledgement required	No AUTACK acknowledgement message expected.
2	Acknowledgement required	An AUTACK acknowledgement message is expected.

4.2.3.5 Filtering function used (0505)

This identifies the filtering function used for validation results and keys. One of the following codes must be used:-

Code	*Meaning*	*Description*
2	Hexadecimal filter	Conversion of hexadecimal data into a character string that is printable, i.e. from each half-byte of data into a one-byte character
6	UN/EDIFACT level EDC filter	Filter function for the UN/EDIFACT character set repertoire C as described in Annex F of Part 5 of ISO 9735
ZZZ	Mutually agreed	An alternative filtering function mutually agreed between the parties involved.

4.2.3.6 Character set of original message (0507)

This identifies the character set in which the message or interchange was coded when security mechanisms were applied. One of the following codes must be used:-

Code	*Meaning*	*Description*
1	ASCII 7 bit	Self explanatory
2	ASCII 8 bit	Self explanatory

Note: if no value is specified, the character set encoding corresponds to that identified by the character set repertoire standard for the interchange as specified in the interchange 'envelope' segments.

4.2.3.7 Security provider role (0509)

This identifies the role that the security provider takes in relation to the secured item. One of the following codes must be used:-

Code	*Meaning*	*Description*
1	Issuer	The security provider is the rightful issuer of the signed document.
ZZZ	Mutually agreed	The role of the security provider is mutually agreed between the parties involved.

Note: when this data element is not used, it is assumed that the security provider is the rightful issuer of the signed document, i.e. the value of 1 is assumed.

4.2.3.8 Security User Id. (0511)

This identifies a party involved in the security process, according to a defined registry of security parties. It is used when keys/certificates do not unambiguously identify the parties involved (see Rules for this segment).

Note 1 - **Security party qualifier (0577)**

This identifies the function or role of the security party identified. One of the following codes ***must*** be used.

Code	*Meaning*	*Description*
1	Message Sender	identifies the party which generates the security parameters of the message (i.e. the security originator)
2	Message Receiver	identifies the party which verifies the security parameters of the message (i.e. the security recipient)

Note 2 - **Security party code list qualifier (0513)**

This is a code that can be used to distinguish between different lists of Security User IDs that are maintained by the same agency (see next note).

Security party code list responsible agency (0515)
This is a code identifying the agency in charge of registration of the security parties.

4.2.3.9 Security time stamp (0338)

This is a security time stamp of the entity to which security is applied. The timestamp is security related and may differ from any dates and times that may appear somewhere else in the entity. It may be used to provide secured entity sequence integrity. It consists of a date in the format CCYYMMDD, and a time in the format HHMMSS where HH is in 24 hour clock format.

Note 3 - **Date and time qualifier (0517)**
This is a code which identifies the type of date/time. The code '1' for Security timestamp ***must always*** be used.

4.2.4 EXAMPLE

USH+7+1+F01+1+2+1+1++++1:19960917:103146'

Component	Meaning	Description
7	Referenced entity non-repudiation of origin	indicates that the security service function is to secure the referenced entity by digital signature to protect against the sender's denial of sending the message.
1	Security reference	this is the 'link no.' which connects the USH segment to its related UST segment
F01	From first transaction message UNH to last transaction message UNT	indicates that the whole set of transaction messages is covered by the scope of the security service function
1	No acknowledgement required	Indicates that the response required is that no acknowledgement is necessary
2	Hexadecimal filter	Indicates that the filtering function used is a hexadecimal filter
1	ASCII 7 bit	Indicates that the character set of the original message is ASCII 7 bit
1	issuer	Indicates that the security provider is the rightful issuer of the signed document
1:19960917 :103146	security timestamp date/time	specifies that the security time stamp is 17th Sept 1996, at 10.31 hrs 46 seconds

4.3 USA SECURITY ALGORITHM (Conditional, Occurs 3, Limited to 1 Required)

4.3.1 This segment identifies a security algorithm, and the technical usage made of it. In addition, the segment contains the technical parameters required.

	Tag #	Description	M/C	*	Format		Code
					USA	+	
	S502	SECURITY ALGORITHM	M	1			
Algorithm usage - owner hashing ⇨	0523	Use of algorithm, coded	M		an..3	:	“1”
	0525	*Cryptographic mode of operation, coded*	*N*		*an..3*	:	
	0533	*Mode of operation code list identifier*	*N*		an..3	:	
Specified algorithm - SHA1 (ISO10118) ⇨	0527	Algorithm, coded	R		an..3	:	“16”
see note 1 ⇨	0529	Algorithm code list identifier	R		an..3	:	“1”
	0591	*Padding mechanism, coded*	*N*		*an..3*	:	
	0601	*Padding algorithm code list identifier*	*N*		*an..3*	+	
	S503	*ALGORITHM PARAMETER*	*N*	*1*			
	0531	*Algorithm parameter qualifier*			*an..3*	:	
	0554	*Algorithm parameter value*			*an..512*	+	
	S503	*ALGORITHM PARAMETER*	*N*	*1*			
	0531	*Algorithm parameter qualifier*			*an..3*	:	
	0554	*Algorithm parameter value*			*an..512*	+	
	S503	*ALGORITHM PARAMETER*	*N*	*1*			
	0531	*Algorithm parameter qualifier*			*an..3*	:	
	0554	*Algorithm parameter value*			*an..512*	+	
	S503	*ALGORITHM PARAMETER*	*N*	*1*			
	0531	*Algorithm parameter qualifier*			*an..3*	:	
	0554	*Algorithm parameter value*			*an..512*	+	
	S503	*ALGORITHM PARAMETER*	*N*	*1*			
	0531	*Algorithm parameter qualifier*			*an..3*	:	
	0554	*Algorithm parameter value*			*an..512*	+	
	S503	*ALGORITHM PARAMETER*	*N*	*1*			
	0531	*Algorithm parameter qualifier*			*an..3*	:	
	0554	*Algorithm parameter value*			*an..512*	+	
	S503	*ALGORITHM PARAMETER*	*N*	*1*			
	0531	*Algorithm parameter qualifier*			*an..3*	:	
	0554	*Algorithm parameter value*			*an..512*	+	
	S503	*ALGORITHM PARAMETER*	*N*	*1*			
	0531	*Algorithm parameter qualifier*			*an..3*	:	
	0554	*Algorithm parameter value*			*an..512*	+	
	S503	*ALGORITHM PARAMETER*	*N*	*1*			
	0531	*Algorithm parameter qualifier*			*an..3*	:	
	0554	*Algorithm parameter value*			*an..512*	’	

4.3.2 RULES

This segment is **not used** in the AUTACK when the message is being used in its acknowledgement role.

4.3.3 DATA REQUIREMENTS

4.3.3.1 Algorithm Usage (0523)

This specifies the use made of the specified algorithm**.** The following code must be used:-

Code	*Meaning*	*Description*
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 non-repudiation of origin identified in the security function qualifier of USH)

4.3.3.3 Specified Algorithm (0527)

This is the algorithm specified for use in this case. The following code must be used.

Code	*Meaning*	*Description*
16	SHA1	Secure Hash Algorithm, Dedicated Hash Function #1; ISO 10118-3

Note 1 **- Algorithm code list identifier (0529)**

It is necessary to specify the code list in which the algorithm is identified. The algorithm identified above comes from the list published by the UN/EDIFACT Security Joint Working Group (SJWG), which is indicated by the code value "1" in this element**.**

4.3.4 EXAMPLE

USA+1:::16:1'

Component	**Meaning**	**Description**
1	Owner hashing	Indicates that the algorithm usage is by the message sender to compute the hash function on the message.
16	SHA1	Indicates that the specified algorithm is the Secure Hashing Algorithm SHA1 detailed in ISO 10118
1	UN/EDIFACT SJWG	Indicates that the list of algorithms is maintained by the EDIFACT Security Joint Working Group.

4.4 to 4.6 Segment Group 2 (Conditional, Occurs 2, Limited to 1)

Tag	*Segment Name*	*M/C*		*Occurs*	
		(1)	*(2)*	*(1)*	*(2)*
Segment group 2 (Conditional, 2)		C			1
USC	Certificate	M		1	
USA	Security Algorithm	C	N	3	0
USR	Security Result	C	N	1	0

Note: (1) indicates the full message specification,
(2) notes any change for this implementation

This segment group contains the data necessary to identify the asymmetric key pair used, even if the certificates are not used.

4.4 USC, SECURITY CERTIFICATE (Mandatory, Occurs 1)

4.4.1 This segment conveys the identity of the public key that is used and also identifies the security party involved.

	Tag #	Description	M/C	*	Format		Code
					USC	+	
	0536	*CERTIFICATE REFERENCE*	*N*	*1*	*an..35*	+	
	S500	SECURITY IDENTIFICATION DETAILS	C	1			
see note 1 ⇨	0577	Security party qualifier	M		an..3	:	
Public Key Name ⇨	0538	Key name	C		an..35	:	
Security Party Id. ⇨	0511	Security party identification	C		an..17	:	
see note 2 ⇨	0513	Security party code list qualifier	C		an..3	:	
	0515	Security party code list responsible Agency, coded	C		an..3	:	
	0586	*Security party name*	*N*		*an..35*	:	
	0586	*Security party name*	*N*		*an..35*	:	
	0586	*Security party name*	*N*		*an..35*	+	
	S500	SECURITY IDENTIFICATION DETAILS	D	1			
see note 1 ⇨	0577	Security party qualifier	M		an..3	:	
Public Key Name ⇨	0538	Key name	C		an..35	:	
Security Party Id. ⇨	0511	Security party identification	C		an..17	:	
see note 2 ⇨	0513	Security party code list qualifier	C		an..3	:	
	0515	Security party code list responsible Agency, coded	C		an..3	:	
	0586	*Security party name*	*N*		*an..35*	:	
	0586	*Security party name*	*N*		*an..35*	:	
	0586	*Security party name*	*N*		*an..35*	+	
	0545	*CERTIFICATE SYNTAX VERSION, CODED*	*N*	*1*	*an..3*	+	
	0505	*FILTER FUNCTION, CODED*	*N*	*1*	*an..3*	+	
	0507	*ORIGINAL CHARACTER SET ENCODING, CODED*	*N*	*1*	*an..3*	+	
	0543	*CERTIFICATE ORIGINAL CHARACTER SET REPERTOIRE, CODED*	*N*	*1*	*an..3*	+	
	0546	*USER AUTHORISATION LEVEL*	*N*	*1*	*an..35*	+	
	S505	*SERVICE CHARACTER FOR SIGNATURE*	*N*	*1*			
	0551	*Service character for signature qualifier*			*an..3*	:	
	0548	*Service character for signature*			*an..4*	+	
	S505	*SERVICE CHARACTER FOR SIGNATURE*	*N*	*1*			
	0551	*Service character for signature qualifier*			*an..3*	:	
	0548	*Service character for signature*			*an..4*	+	
	S505	*SERVICE CHARACTER FOR SIGNATURE*	*N*	*1*			
	0551	*Service character for signature qualifier*			*an..3*	:	
	0548	*Service character for signature*			*an..4*	+	
	S505	*SERVICE CHARACTER FOR SIGNATURE*	*N*	*1*			
	0551	*Service character for signature qualifier*			*an..3*	:	
	0548	*Service character for signature*			*an..4*	+	

S505 *0551* *0548*	*SERVICE CHARACTER FOR SIGNATURE* *Service character for signature qualifier* *Service character for signature*	*N*	*1*	 *an..3* *an..4*	 : +	
S501 *0517* *0338* *0314* *0336*	*SECURITY DATE AND TIME* *Date and time qualifier, coded* *Event date* *Event time* *Time offset*	*N*	*1*	 *an..3* *n..8* *an..15* *n4*	 : : : +	
S501 *0517* *0338* *0314* *0336*	*SECURITY DATE AND TIME* *Date and time qualifier, coded* *Event date* *Event time* *Time offset*	*N*	*1*	 *an..3* *n..8* *an..15* *n4*	 : : : +	
S501 *0517* *0338* *0314* *0336*	*SECURITY DATE AND TIME* *Date and time qualifier, coded* *Event date* *Event time* *Time offset*	*N*	*1*	 *an..3* *n..8* *an..15* *n4*	 : : : +	
S501 *0517* *0338* *0314* *0336*	*SECURITY DATE AND TIME* *Date and time qualifier, coded* *Event date* *Event time* *Time offset*	*N*	*1*	 *an..3* *n..8* *an..15* *n4*	 : : : +	
0567	*SECURITY STATUS*	*N*	*1*	*an..3*	+	
0569	*REVOCATION REASON, CODED*	*N*	*1*	*an..3*	’	

4.4.2 RULES

4.4.3 DATA REQUIREMENTS

4.4.3.1 Public Key Name (0538)

This identifies the public key of the identified security party.

4.4.3.2 Security Party Id. (0511)

This is a code identifying a party involved in the security process, according to a defined registry of security parties. It may be either:-

- the party which owns the certificate or named public key, or
- the party which certifies that the document (i.e. the certificate) is authentic, the Authenticating Party or Certification Authority.

Note 1 - **Security party qualifier (0577)**

This specifies the role or function of the security party described above. One of the following codes must be used:-

Code	*Meaning*	*Description*
3	Certificate Owner	identifies the party as the owner of the certificate.
4	Authenticating Party	identifies the party as the one which certifies that the document (i.e. the certificate) is authentic.

Note 2 - **Security party code list qualifier (0513)**

This is a code identifying the type of identification used to register the security parties.

Security party code list responsible agency (0515)
This is a code identifying the agency in charge of registration of the security parties.

4.4.4 EXAMPLE

USC++3:KEY10:5016622123456::9’

Component	Meaning	Description
3	Certificate owner	Indicates that the security party identified is the one which owns the certificate
KEY10	Public key name	identifies the public key of the identified security party. As the security party has been identified as the authenticating party, this is the public key related to the secret key used by them to sign the referenced certificate.
5016622123456	Security party id.	a code identifying the party, in this case an EAN-13 id. from…
9		... the registry maintained by EAN International.

4.5 USA SECURITY ALGORITHM (Conditional, 3) ** not used **

4.6 USR SECURITY RESULT (Conditional, 1) ** not used **

4.7 USB, SECURED DATA IDENTIFICATION (Mandatory , Occurs 1)

4.7.1 This segment identifies the interchange sender and recipient, and contains the date/time of creation, of the AUTACK message. It must specify whether or not a secure acknowledgement is required from the recipient. If one is required, the message sender will expect an AUTACK acknowledgement message to be sent back by the message recipient. The interchange sender and recipient identified in the USB must be the sender and the recipient of the interchange in which the AUTACK is present.

	Tag #	*Description*	*M/C*	*	*Format*		*Code*
					USB	+	
Secure response required ⇨	0503	RESPONSE TYPE,CODED	M	1	an..3	+	
	S501	SECURITY DATE AND TIME	R	1			
see note 1 ⇨	0517	Date and time qualifier	M		an..3	:	
Generation date/time ⇨	0338	Event date	R		n..8	:	
	0314	Event time	R		an..15	:	
	0336	*Time offset*	*N*		*n4*	+	
	S002	INTERCHANGE SENDER	M				
Interchange Sender Id. ⇨	0004	Interchange sender identification	M		an..35	:	
see note 2 ⇨	0007	Identification code qualifier	C		an..4	:	
	0008	*Interchange sender internal Identification*	*N*		*an..35*	:	
	0042	*Interchange sender internal sub-Identification*	*N*		*an..35*	+	
	S003	INTERCHANGE RECIPIENT	M				
Interchange Receiver Id. ⇨	0010	Recipient identification	M		an..35	:	
see note 3 ⇨	0007	Identification code qualifier	C		an..4	:	
	0014	*Interchange recipient internal Identification*	*N*		*an..35*	:	
	0046	*Interchange recipient internal sub-Identification*	*N*		*an..35*	’	

4.7.2 RULES

4.7.3 DATA REQUIREMENT

4.7.3.1 Response required (0503)

This specifies whether a secure acknowledgement from the message recipient is required or not. If it is required, the message sender expects an AUTACK message to be sent back by the current message recipient to the current message sender, containing this acknowledgement**.** One of the following codes must be used:-

Code	*Meaning*	*Description*
1	No acknowledgement required	No AUTACK acknowledgement message expected.
2	Acknowledgement required	An AUTACK acknowledgement message is expected.

4.7.3.2 Generation date/time (0338)

This is the date/time when the AUTACK was generated. It consists of a date in the format CCYYMMDD, and a time in the format HHMMSS where HH is in 24 hour clock format.

Note 1 - **Date and time qualifier (0517)**

This is a code that identifies the type of date/time. One of the following ***must always*** be used.

Code	Name	Description
5	Generation date/time	identifies the date/time as that when the AUTACK itself was generated
1	Security Timestamp	identifies the date/time as a security timestamp

4.7.3.3 Interchange Sender Id. (0004)

This is a coded identification of the party sending the interchange that contains the AUTACK, and is taken from the interchange's UNB.

Note 2 - **Identification code qualifier (0007)**

This is a code that identifies the scheme of party identification that is used for the interchange sender.

4.7.3.4 Interchange Receiver Id. (0010)

This is a coded identification of the party receiving the identified interchange that contains the AUTACK, and is taken from the interchange's UNB.

Note 3 - **Identification code qualifier (0007)**

This is a code that identifies the scheme of party identification that is used for the interchange receiver.

4.7.4 EXAMPLE

USB+1+5:19960917:084453+9988776655:9+1122334455:9’

Component	Meaning	Description
1	No acknowledgement required	indicates that a secure acknowledgement is not required in response
5	Date of AUTACK creation	indicates that the date which follows is the date when the AUTACK was created
19960917:084453		Specifies the date of 17th Sept 1996, at the time of 08.44 hrs and 53 seconds
9988776655:9	Interchange sender id.	Identifies the interchange sender by a coded id., maintained in this case by EAN International
1122334455:9	Interchange receiver id.	Identifies the interchange recipient by a coded id. , maintained in this case by EAN International

4.8 to 4.9 Segment Group 3 (Mandatory, Occurs 9999, Limited to 1)

Tag	*Segment Name*	*M/C*		*Occurs*	
		(1)	*(2)*	*(1)*	*(2)*
Segment group 3 (Mandatory, 9999)					1
USX	Security Reference	M		1	
USY	Security on Reference	M		9	2

Note: (1) indicates the full message specification,
(2) notes any change for this implementation

This group is used to identify an EDIFACT structure in the security process and to give security information on the referenced structure.

4.8 USX, SECURITY REFERENCES (Mandatory, Occurs 1)

4.8.1 This segment refers to the secured interchange and its associated date and time.

		Tag #	*Description*	*M/C*	*	*Format*		*Code*
Referenced Entity:-						**USX**	+	
Interchange Id. No.	⇨	0020	INTERCHANGE CONTROL REFERENCE	R	1	an..14	+	
		S002	INTERCHANGE SENDER	C	1			
Interchange Sender Id.	⇨	0004	Interchange sender identification	M		an..35	:	
See note 1	⇨	0007	Identification code qualifier	C		an..4	:	
		0008	Interchange sender internal Identification	C		an..35	:	
		0042	Interchange sender internal sub-Identification	C		an..35	+	
		S003	INTERCHANGE RECIPIENT	C	1			
Interchange Recipient Id.	⇨	0010	Interchange recipient identification	M		an..35	:	
See note 2	⇨	0007	Identification code qualifier	C		an..4	:	
		0014	Interchange recipient internal Identification	C		an..35	:	
		0046	Interchange recipient internal sub-id.	C		an..35	+	
		0048	*GROUP REFERENCE NUMBER*	*N*	*1*	*an..14*	+	
		S006	*APPLICATION SENDER IDENTIFICATION*	*N*	*1*			
		0040	*Application sender identification*	*N*		*an..35*	:	
		0007	*Identification code qualifier*	*N*		*an..4*	+	
		S007	*APPLICATION RECIPIENT ID.*	*N*	*1*			
		0044	*Application recipient identification*	*N*		*an..35*	:	
		0007	*Identification code qualifier*	*N*		*an..4*	+	
		0062	*MESSAGE REFERENCE NUMBER*	*N*	*1*	*an..14*	+	
		S009	*MESSAGE IDENTIFIER*	*N*	*1*			
		0065	*Message type*			*an..6*	:	
		0052	*Message version number*			*an..3*	:	
		0054	*Message release number*			*an..3*	:	
		0051	*Controlling agency*			*an..2*	:	
		0057	*Association assigned code*			*an..6*	:	
		0110	*Code list directory version number*			*an..6*	:	
		0113	*Message type sub-function identification*			*an..6*	+	
		0800	*PACKAGE REFERENCE NUMBER*	*N*	*1*	*an..14*	+	
		S501	SECURITY DATE AND TIME	C	1			
See note 3	⇨	0517	Date and time qualifier	M		an..3	:	
Origin Date/time	⇨	0338	Event date	C		n..8	:	
	⇩	0314	Event time	C		an..15	:	
		0336	*Time offset*	*C*		*n4*	'	

4.8.2 RULES

4.8.3 DATA REQUIREMENT

4.8.3.1 Interchange Id. No. (0020)

This contains the unique identification assigned by the sender to the interchange that is referred to as the subject of the AUTACK message, i.e. the Interchange ID No. of that interchange.
In the authentication AUTACK that accompanies the secured interchange it will be the Interchange ID No. from the UNB in which the AUTACK is placed
In the acknowledgement AUTACK it will be the Interchange ID No. from the UNB of the original interchange that the AUTACK is acknowledging.

4.8.3.2 Interchange Sender Id. (0004)

This is a coded identification of the party sending the interchange to which this AUTACK refers.

Note 1 - **Identification code qualifier (0007)**

This is a code which identifies the scheme of party identification that is used for the interchange sender.

4.8.3.3 Interchange Receiver Id. (0010)

This is a coded identification of the party receiving the interchange to which this AUTACK refers.

Note 2 - **Identification code qualifier (0007)**

This is a code which identifies the scheme of party identification that is used for the interchange receiver.

4.8.3.4 Origin Date/time (0338)

This is the date and time when the referenced EDIFACT interchange was created. It consists of a date in the format CCYYMMDD and, when necessary, a time in the format HHMMSS where HH is in 24-hour clock format.

Note 3 - **Date and time qualifier (0517)**

This is a code that identifies the type of date/time. The following ***must always*** be used.

Code	Name	Description
5	Generation date/time	identifies the date/time as that when the referenced entity was created

4.8.4 EXAMPLE

USX+1007++++++++5:19970916:153051’

Component	Meaning	Description
1007	Interchange control reference	Gives the identity of the interchange that is the subject of this AUTACK message.
5:19970916: 153051’	Origin date/time	Indicates the date/time of origination of the subject as 16th Sept.1997, at 15.30hrs +51 secs.

4.9 USY, SECURITY ON REFERENCES (Mandatory, Occurs 9, Limited to 2)

4.9.1 This segment identifies the security header that contains the security specifications, such as the algorithm used, by a 'link number'. The segment contains the authenticating digital signature.

		Tag #	*Description*	*M/C*	*	*Format*		*Code*
						USY	+	
Link Number	⇨	0534	SECURITY REFERENCE NUMBER	M	1	an..14	+	
		S508	VALIDATION RESULT	R	1			
see note 1	⇨	0563	Validation value qualifier	M		an..3	:	"1"
Digital signature of Referenced interchange	⇨	0560	Validation value	C		an..512	+	
		S508	*VALIDATION RESULT*	*N*	*1*			
		0563	*Validation value qualifier*			*an..3*	:	
		0560	*Validation value*			*an..512*	+	
		0571	*SECURITY ERROR, CODED*	*N*	*1*	*an..3*	'	

4.9.2 RULES

4.9.3 DATA REQUIREMENT

Only one occurrence of the validation result S508 is needed as the algorithm recommended produces a one-part result, unlike some other algorithms.

4.9.3.1 Link Number (0534)

This security reference number links a particular USY segment with its corresponding USH segment, the value used is arbitrarily assigned. Within one message the same value cannot be re-used to identify another different set.

4.9.3.2 Digital signature (0560)

This contains the security result corresponding to the security functions specified in the Filter Function of the linked USH segment and in the USC group's USA where the digital signature algorithm is indicated.

The length of this data element is determined by the length of the key (one of the digital signature algorithm parameter data elements, qualified by the algorithm parameter qualifier 'modulus length', of the owner signature algorithm) and the filter function applied to the result of the signature process.

Note 1 **- Validation value qualifier (0563)**

This distinguishes the different instances of validation value. The following code must be used:-

Code	*Meaning*	*Description*
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 (e.g. one MAC with DES algorithm)

4.9.4 EXAMPLE

USY+1+1:ABF0F984BCD909E4BCDA1871AACCBBEDFF3FF43183EDFFA’

Component	Meaning	Description
1	Security reference number	specifies the link reference number that ties this USY segment to its related USH segment
1	Unique validation value	indicates that the validation value which follows is for use of authentication
ABF0F9...3EDFFA	Validation value	gives the security result that corresponds to the security function specifed in the linked USH segment, in this case a digital signature (see USH example)

4.10 to 4.11 Segment Group 4 (Mandatory, Occurs 99, Limited to 2)

Tag	*Segment Name*	*M/C*		*Occurs*	
		(1)	*(2)*	*(1)*	*(2)*
Segment group 4 (Mandatory, 99)					2
UST	Security Trailer	M		1	
USR	Security Result	C	N	1	0

Note: (1) indicates the full message specification,
(2) notes any change for this implementation

A 'link number' connects this group of segments to its related security header group. It is also linked in the same way to the security result group.

4.10 UST, SECURITY TRAILER (Mandatory, Occurs 1)

4.10.1 This segment establishes a link between the security header and the security trailer. It also gives a count of segments for simple checking purposes.

		Tag #	*Description*	*M/C*	*	*Format*		*Code*
						UST	**+**	
Link Number	⇨	0534	SECURITY REFERENCE NUMBER	M	1	an..14	+	
Count of Security Segments	⇨	0588	NUMBER OF SECURITY SEGMENTS	M	1	n..10	**'**	

4.10.2 RULES

4.10.3 DATA REQUIREMENT

4.10.3.1 Link Number (0534)

This reference number links a particular UST segment with its corresponding USH segment, the value used is arbitrarily assigned but, within one message, the same value must not be used more than once.

4.10.3.2 Count of Security Segments (0588)

This is the count of segments which have been used in the security 'set', i.e. all the segments in groups connected by the same link number. This would include all segments of groups 1, 2, and 4 for which the link number in USH, and UST is the same. It is intended to give the recipient a simple control check between the number of segments sent in the set and the number received.

4.10.4 EXAMPLE

UST+1+4'

Component	Meaning	Description
1	Security reference number	specifies the link reference number that ties this UST segment to its related USH segment and USY segment
4	Count of security segments	specifies that there are four segments in the security set (i.e. the linked USH with its USA,USC, and the UST) which are linked by the same value in 'link number'

4.11 USR, SECURITY RESULT (Conditional, 1) ** not used **

4.12 UNT, MESSAGE TRAILER (Mandatory, 1)

4.12.1 This segment specifies the end of the message. It indicates the total number of segments and the sequential reference number of the message, as quoted in the Message Header (UNH) segment.

		Tag #	*Description*	*M/C*	*	*Format*		*Code*
						UNT	+	
Count of segments	⇨	0074	NUMBER OF SEGMENTS IN MESSAGE	M		n..6	+	
Message ID. No.	⇨	0062	MESSAGE REFERENCE NUMBER	M		an..14	’	

4.12.2 RULES

4.12.3 DATA REQUIREMENT

4.12.3.1 Number of Segments in a Message (0074)

This specifies the total number of segments, starting with the Message Header (UNH) segment and ending with the Message Trailer (UNT) segment, which have been used in the message. This information will provide the receiver of the message with a control count to ensure that the entire message has been received.

4.12.3.2 Message Reference Number (0062)

This number is the same as the message reference number of the message quoted in the Message Header (UNH) segment. It is the unique message reference number within a range of messages sent. Numbers ***must*** be allocated in ascending sequence order within an interchange (e.g. the first message sent is 001, the second 002,etc.)

4.12.4 Example

UNT+9+11'

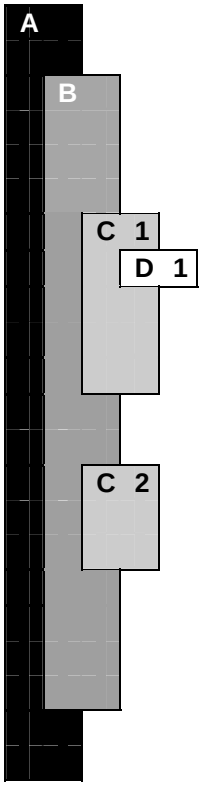
Component	Name	Description
9	Number of Segments in a message	There are nine segments, including the UNH and UNT, in the message transmitted.
11	Message Reference Number	Control reference number of the message; it is an exact repeat of the Message Reference Number that appears in the UNH Message Header segment.

5. Message Format Specifications

5.1 Segment Listing

This overview shows the segments and segment groups of the full AUTACK message.

In the simplified usage that this document describes, some parts of the AUTACK message are not used. The 'M/C' columns indicate whether or not the segment or group is necessary, M indicating it is mandatory and C that it is conditional in the full message. The R indicates that it is needed, and N that it is not used, in this simplified usage. The first 'occurs' columns indicates the number of times a segment or segment group can occur in the full message, while the second shows that this is limited within the simplified usage described in Chapter 4. The 'see 4.n' column indicates the section in Chapter 4 where the segment is described.



	Tag	*Data Segment Name*	*M/C (1)*	*(2)*	*Occurs (1)*	*(2)*	*See 4.n*
A	UNH	Message Header	M		1		4.1
B		**Segment Group 1**	M		99	2	
	USH	Security Header	M		1		4.2
	USA	Security Algorithm	C	R	3	1	4.3
C 1		**Segment Group 2**	C	C	2	1	
D 1	USC	Certificate	M		1		4.4
	USA	*Security Algorithm*	*C*	*N*	*3*	*0*	*4.5*
	USR	*Security Result*	*C*	*N*	*1*	*0*	*4.6*
	USB	Secured Data Identification	M		1		4.7
C 2		**Segment Group 3**	M		9999	1	
	USX	Security References	M		1		4.8
	USY	Security on References	M		9	2	4.9
		Segment Group 4	M		99	2	
	UST	Security Trailer	M		1		4.10
	USR	*Security Result*	*C*	*N*	*1*	*0*	*4.11*
	UNT	Message Trailer	M		1		4.12

Note that there is no structural link connecting the security header (segment group 1), the security trailer (segment group 4), the item being secured and the digital signature (segment group 3). A 'link number' is used for each separately secured 'set' of information, i.e. all the instances of segment groups 1-4 that relate together.

In general terms, the message is used in the following simplified way:-

5.1.1 For Authentication

The authentication AUTACK uses one occurrence of the USX 'Security References' segment to reference the interchange that it authenticates. With the USX segment there shall be one corresponding USY 'Security on References' segment and this contains the security result, i.e. the digital signature computed on the hash value of the referenced interchange.

Details about the security functions performed shall be contained in the AUTACK security header group, i.e. ‘B’ in the diagram. One occurrence of the USA segment following the USH is used to indicate the hash algorithm used. The USC segment is used to refer to the pre-arranged set of keys that are being used. One USA segment following the USC is used to indicate the digital signature algorithm used.

The USY and USH segments for the referenced EDIFACT structure shall be linked using the ‘link reference’ which is in both segments. Although this is logically unnecessary, given only one occurrence of USH and USK is used, the design of the message insists on it being present.

As defined in EDIFACT security documentation ISO9735 Part 6, the AUTACK itself does not need to be secured because it conveys a digital signature.

Example AUTACK with double signature:-

UNH+*message number*+AUTACK:3:1:UN:SECAUT'
USH+7+1+F01+1+2+1+1++++1:*date stamp*:*time stamp*'
USA+1:::16:1'
USC++3:*first public key name*:*security party id*'
USH+7+2+F01+1+2+1+1++++1:*date stamp*:*time stamp* '
USA+1:::16:1'
USC++3:*second public key name*:*security party id*'
USB+1+5:*AUTACK generation date*:*time*+*interchange sender id*+ *interchange receiver id* '
USX+*secured interchange id*++++++++5:*Origin date*:*time*'
USY+1+1:*first digital signature*'
USY+2+1:*second digital signature* '
UST+1+4'
UST+2+4'
UNT+14+*message number* '

The italicised entries are where the named piece of data is entered. These are pieces which typically would vary on each occasion while the rest is always the same.

5.1.2 For Acknowledgement

The acknowledgement AUTACK uses one occurrence of the USX 'Security References' segment to reference the original I nterchange that it is acknowledging. With the USX segment there shall be one corresponding USY 'Security on References' segment which contains the security result, i.e. the digital signature of the recipient of the original interchange computed on the hash value of the original interchange.

Details about the security functions performed shall be contained in the AUTACK security header group, i.e. ‘B’ in the diagram. The USC segment is used to refer to the pre-arranged set of keys that are being used by the acknowledgement sender.

The USY and USH segments for the referenced EDIFACT structure shall be linked using the ‘link reference’ which is in both segments. Although this is logically unnecessary, given only one occurrence of USH and USY is used, the design of the message insists on it being present.

As defined in EDIFACT security documentation ISO9735 Part 6, the AUTACK itself does not need to be secured because it conveys a digital signature.

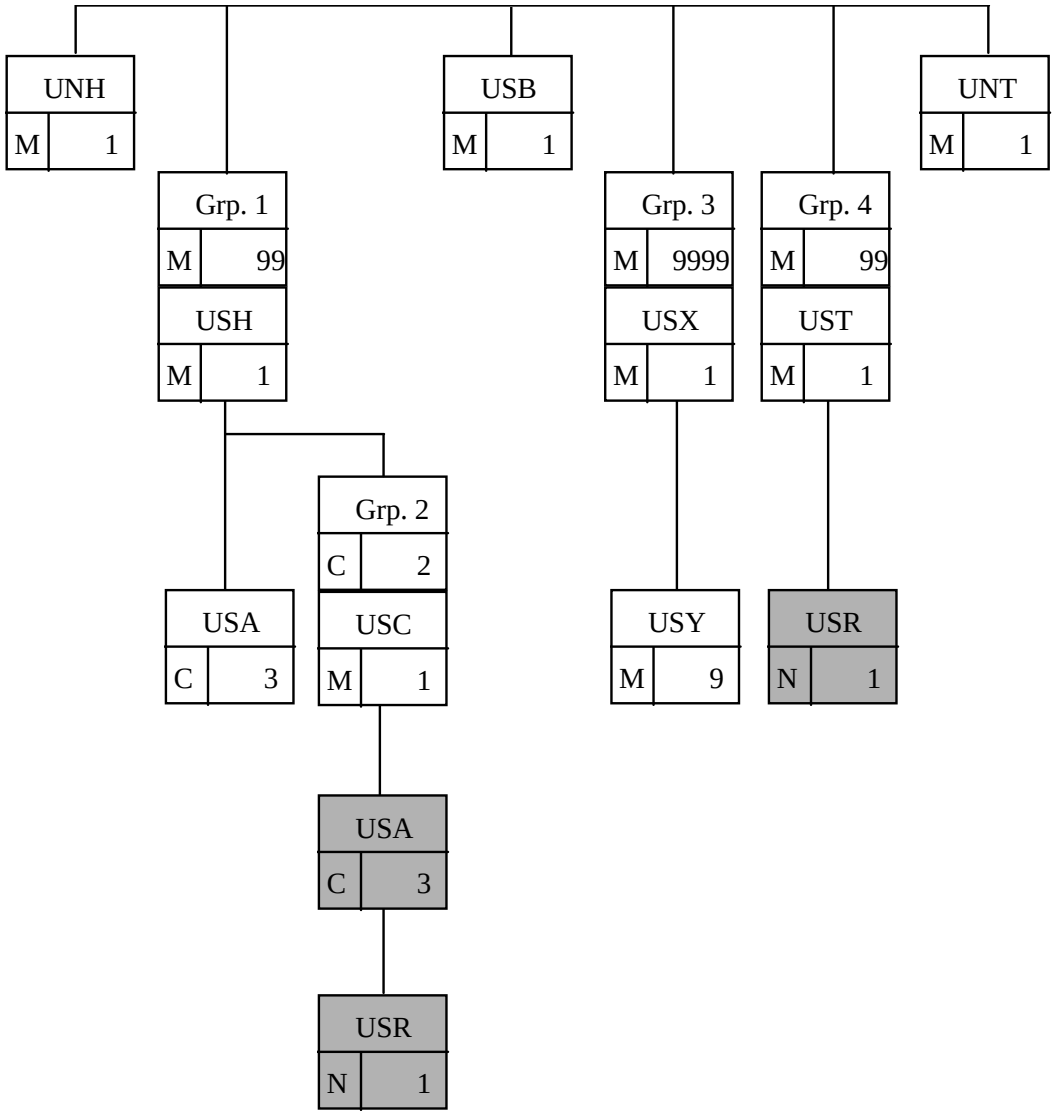
Example:-

UNH+*message number*+AUTACK:3:1:UN:SECACK'
USH+5+1+F01+1+2+1+1++++1:*date stamp*:*time stamp*'
USC++3:*public key name*:*security party id*'
USB+1+5:*AUTACK generation date*:*time*+*interchange sender id*+ *interchange receiver id* '
USX+*secured interchange id*++++++++5:*Origin date*:*time*'
USY+1+1:*digital signature*'
UST+1+4'
UNT+8+ *message number* '

The italicised entries are where the named piece of data is entered. These are pieces that typically would vary on each occasion while the rest is always the same. Note that, in this context *secured interchange id* relates to the original secured interchange that is being acknowledged and the *public key name* and *security party id.* relate to the original interchange's receiver.

5.2 Branching Diagram

This gives the same information for the full message as it appears in the previous section 5.1 but presented in a graphical form.



Shaded segments are not used in this specification.