DIGITAL SIGNATURE FOR EANCOM MESSAGES

GS1 Implementation Guidelines

EANCOM TDT

DOCUMENT v1.0

TABLE OF CONTENTS

1 Introduction

GS1 is committed to facilitate business relations between trading partners through the development of agreed standards for the identification of products and locations, and communications EDI). In the area of communication, the use of the EDI standard EANCOM® (fully compliant subset of UN/EDIFACT) has become the most popular tool for international electronic trade covering activities such as purchasing, transport and finance. Since EANCOM® deals with the trade of goods, safeguards must be provided to protect trading partner relations and most importantly, the data exchanged.

Economic tendencies towards electronic business carried out over non-secure networks (such as Internet) require the use of additional measures to protect the information being sent and received. In order to successfully conduct any business activity over the net, a company should be considered by the consumers as a trusted entity that protects their identity and personal data (i.e. home address, credit card number, …). The use of the digital signature, an optionally encryption techniques, within business boundaries and activities, constitutes a true value added tool and service that provides end-users with the enough degree of confidence towards the transactions they are involved in.

GS1 has developed the following guide on how to secure EANCOM® messages to highlight some possible safeguards available within the UN/EDIFACT standard. The decision to use security solutions in an EDI environment will depend on the data exchanged and the potential losses which might occur through the accidental or malicious corruption of a message.

There are others way to digitally sign and protect an EDIFACT document related to usage of specifics transports protocols, such as EDIINT AS1, AS2, S/MIME and others which are out of scope of this document.

2 Objective of the Document

The objective of the document is to describe the EANCOM® application functionalities to secure - digital signature - electronic transactions based on EDIFACT messages. The scope of EDI security in this document covers the flow of information between leaving the message sender's secure EDI gateway, and its arrival at the trading partner's secure EDI gateway.

3 Digital Signature: Benefits

The use of the digital signature technique in EANCOM® messages brings forward different value added services. Regarding to the electronic exchange over the net, Digital Signature techniques represent a real countermeasure and security solution to protect the information against most common threats. The use of the digital signature avoids:

- **Content Integrity**

  This solution protects against modification of the data exchanged.

  The sender applies an algorithm to the message before sending it to obtain an integrity control value that is included with in the message. The receiver applies the same algorithm to the received message (following the corresponding instructions) and the result must match the integrity value sent.

- **Origin Authentication**

  This solution protects the receiver against processing the data from a party claiming to be another party.

  Authentication codes are transmitted within the message to the receiver to ensure the identity of the sender. These authentication codes (digital certificate) are generated by a third authorised and trusted agent (Authority of Certification) and SHOULD be exchanged between the trading partners before any transaction takes place. The receiver validates that the digital signature values match the authentication codes contained in the digital certificate.

- **Non-repudiation of Origin**

  This solution protects the receiver of the message from the sender's denial of having sent the message.

  The sender digitally signs the message. The receiver uses the check code contained in the digital signature and the certificate associated to the sender to validate the message. Hence, if the message is valid, the sender must have sent it. There is no possibility that another party had generated that message without getting an error during the verification process.

- **Non-repudiation of Receipt (if a response message is implemented)**

  This solution protects the sender of a message from the receiver's denial of having received the message.

  The sender must request an acknowledgement from the receiver that the message has been received. The receiver should include with the acknowledgement a digital signature to guarantee the integrity of the acknowledge message and to authenticate the receivers identity.

  The digital signature ensures the *integrity* of the message, the *authentication* of the involved parties and the *non-repudiation* of the message.

The decision of using digital signature techniques will depend, ultimately, on the type of information that is going to be exchanged and the number of potential threats that intentionally or accidentally might damage the transmitted information.

4 EDIFACT Security Rules

For a full description of the way to implement Security in EDIFACT Messages, have a look at ISO 9375. In this point we are going to describe the Key points to manage security (Digital Signature):

4.1 *Digital Signature*

For the Digital Signature process, EDIFACT allows two different ways to generate the digital signature:

- Include the Digital Signature inside the EDIFACT Document (Attached) - Security headers and trailers.
- Include the Digital Signature in a separate EDIFACT Document: AUTACK Message (Detached).

Both of them are for EDIFACT Syntax 4 messages and Security Headers and Trailers must be used to carry the information related to security.

4.2 *Attached vs Detached*

The use of Attached Digital Signatures versus Detached Digital Signatures has been widely discussed in EANCOM® TDT with the following conclusions:

Where the Attached Method is better:

- Autack delayed reception
  The original document and signature might not arrive at the same time at the receiver. There are many applications and cases (legal constraints, …) that imply that signature validation is required before processing the document (i.e. in digital signatures it is mandatory to verify signature before accept the invoice content). In those cases, the document processing must be paused and delayed until AUTACK reception takes place. When using attached signature all the information is send at once, so it is not possible to receive one part without the other one.

  If there is no constraint on the reception process, that is, it is not necessary to verify signature before processing the document. In this particular case, after reception of the document (but not the AUTACK) the application begins to process it (i.e. send to ERP…).

  After the mapping takes place, the message is stored in a database and removed from the EDI-software.

- Message delayed reception
  Indeed, if we use detached signature it might also be possible to receive an AUTACK but not the document associated to it. This case is just the other way around of the aforementioned bullet. Again, we need to 'define' a new process status ('paused until reception of document') that generates an additional cost to reception processes.

  When using attached signature all the information is send at once, so it is not possible to receive one part without the other

- Ambiguity
  Note that the scenario explained in 2 paragraph of first bullet (i.e. reception of the original document and processing of it. After storage, we remove it from the EDI software. When we receive the AUTACK, we can not link both messages), could be easily solved by defining that the original document can not be removed until reception of AUTACK. But this is not as easy as it seems. Why? Because we don't have a clue to decide which documents need to wait for an AUTACK and which ones do not. So, how can we sort them? There is no way at all.

- Incompleteness
  There are many cases where digital signature is extremely important. If we send a digital invoice digitally signed, the signature is an essential part of the e-invoice. In fact, if the signature is removed, the document is not valid from a legal point of view

  By using detached signatures it might happen that original message is received but the AUTACK message never arrives.

- Storage

It is easier to store a single document (attached) that two different documents linked by a number (detached).

Where the Detached Method is better:

- The main advantage of using the AUTACK message is that the EANCOM® message/interchange stays the same (e.g. based on current recommendations EANCOM® 97/2002 Syntax 3). There is no need to change the Directory nor Syntax of message being sent at the moment.

Even if both methods detailed above are valid, the usage of **Attached Method** is recommended by EANCOM TDT. This document will show how to use the Attached and Detached Method of digital signature in EANCOM® messages.

4.3 *AUTACK Message*

AUTACK is a message authenticating sent, or providing secure acknowledgement of received interchanges, groups, messages or packages.

A secure authentication and acknowledgement message can be used to:

a) Give secure authentication, integrity or non-repudiation of origin to messages, packages, groups or interchanges.
b) Give secure acknowledgement or non-repudiation of receipt to secured messages, packages, groups or interchanges. The AUTACK Message then must be secured.

An AUTACK message used as an acknowledgement message shall be sent by the recipient of one or more previously received secured EDIFACT structures, or by a party having authority to act on behalf of the recipient. Its purpose is to facilitate confirmation of receipt, validation of integrity of content, validation of completeness and/or non-repudiation of receipt of its associated EDIFACT structures.

The acknowledgement function shall be applied only to secured EDIFACT structures. The secured EDIFACT structure shall be referenced in an occurrence of the USX (security references) segment. For each USX there shall be at least one corresponding USY (security on references) segment which contains either the hash value or the digital signature of the referenced EDIFACT structure. The USY shall be linked to a security header group of the referenced EDIFACT structure, or of an AUTACK message securing it, by using security reference number data element. The corresponding security header related to the referenced EDIFACT structure contains the details of the security function performed on the referenced EDIFACT structure by the sender of the original message

As a final step in generation of the acknowledgement message, all the information conveyed in the AUTACK shall be secured using at least one pair of security header and security trailer groups.

AUTACK may also be used for non-acknowledgement in case of problems with the verification of the security results.

To prevent endless loops, an AUACK used for the acknowledgment function shall not require its recipient to send back an AUTACK acknowledgement message.

4.4 *Digital Certificates*

Digital Certificates are issued by a trusted third party known as a Certification Authority (CA). When an individual provides information to the CA as part of the online application process, the CA verifies the information and issues a Digital Certificate to the individual (Subscriber). In so doing, the CA attests to the fact that the individual is in fact the person named in the Certificate. Somewhat like a passport, the Certificate can be presented to Internet trading partners to provide proof of identity.

A Digital Certificate is an electronic credential that allows an individual to prove their identity during online transactions. It forms the basis by which an individual can create a "digital signature" for use in electronic transactions, thereby eliminating the need for paper.

Different formats for Digital Certificates exist in the market, however, X.509v3 Digital Certificates are the ones used in B2B transactions and deliver by all Trusted Certification Authorities.

There are two different ways to exchange the digital certificates:

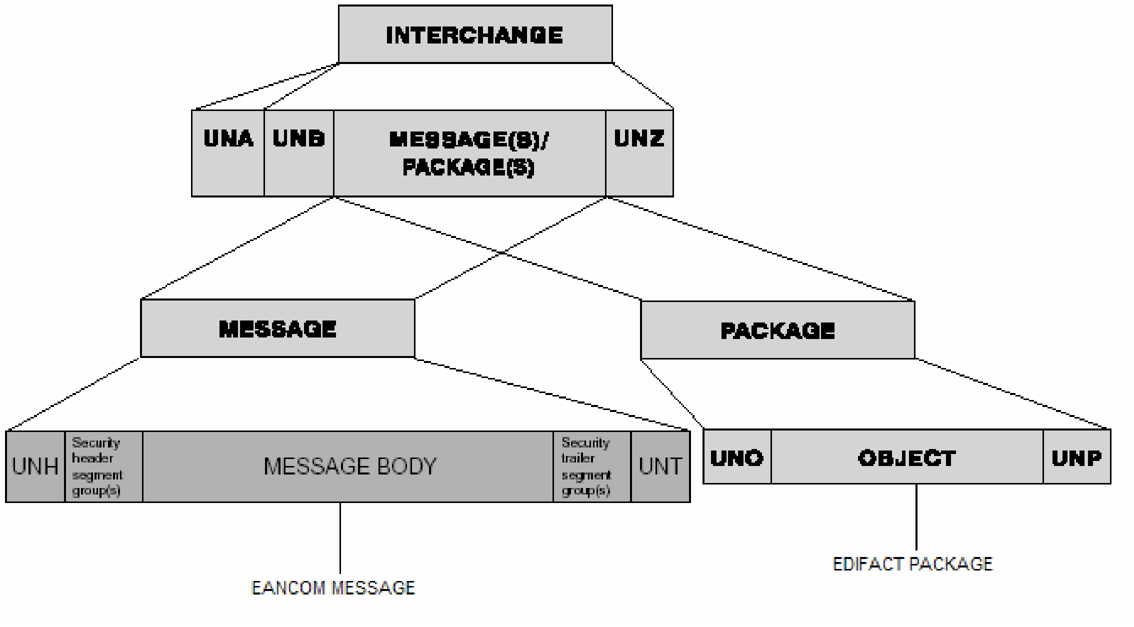
- Inside the EANCOM® interchange using EDIFACT packages
- By other means: e-mail, disks, download from website, …

Digital Certificates following EDIFACT Certificate Structure can be detailed inside the Security Header. Digital Certificates not following EDIFACT Certificate Structure can not be indicated in the Security Header and must be conveyed in an EDIFACT package.

The way to convey an EDIFACT package inside an EDIFACT document is detailed in ISO9735-8. The use of EDIFACT packages will allow including binary objects (i.e. digital certificates X.509v3 and other), inside an interchange. EDIFACT package is the equivalent to the "attached file" in an e-mail.

4.5 *Interchange Structure including Security according to EDIFACT*

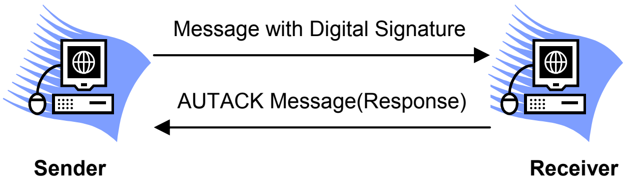
The following picture shows the structure of an EDIFACT Document with Digital Signature and a Package conveyed.



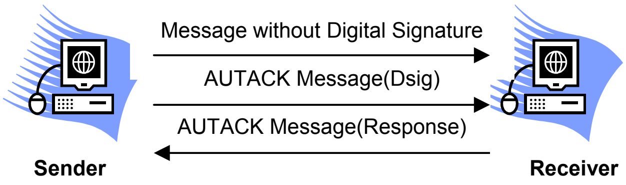
Different messages to be included in an interchange: segments UNH-UNT. An object can optionally be attached before the interchange ends, Segments UNO-UNP.

4.6 *Message Choreography*

Message choreography for attached and detached digital signatures is detailed in the next picture:



Message Choreography – Attached Digital Signature



Message Choreography –Detached Digital Signature

It is up to the trading partners to decide if they want to use the AUTACK message as a response message. It is highly recommended that even if the trading partners have agreed not to use it, to be sent in case of the digital signature validation process fails.

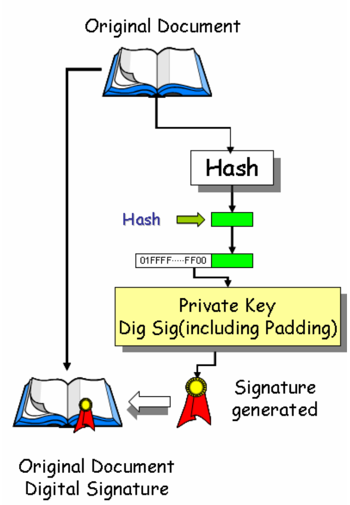
5 Main Parameters in the signature process

The objective of this point is to analyse the algorithms related to security that will take part in the digital signature process.

5.1 *Schema of the Digital Signature Process*

5.1.1 Generation of the Digital Signature

The process to generate the digital signature for an EANCOM document is shown below:



Once we have the EANCOM document, the Hash digest is calculated. The value coming from the Hash algorithm is processed with the private key of the sender to get the result of the digital signature process (including the padding process)

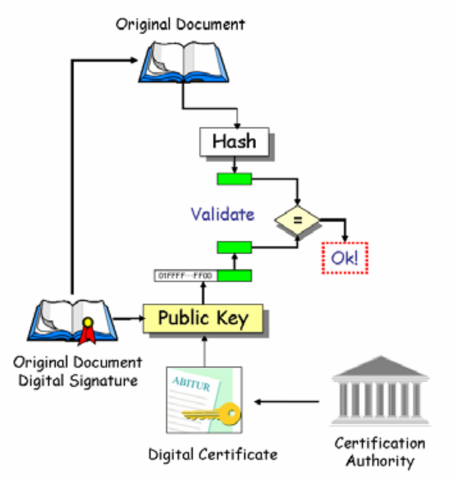
The result of the digital signature process must be placed in the right segment in the EANCOM message and the Security Header/Trailer must be built.

Digital Signature Creation Process

Once the document is digitally signed it is ready to be sent to the trading partner. The Sending Party sends the document with the result of the digital signature process.

5.1.2 Validation of the Digital Signature

The process to validate the digital signature for an EANCOM document is shown below:



Digital Signature Validation Process

The receiver of the document uses the public key of the sender to get the result of the hash algorithm.

The receiver takes the original message and gets the hash value.

To know if the document was correctly signed, the receiver will compare the hash obtained from the original message and the one obtained after processing the digital signature value. If value is the same then the validation process succeeded.

Once the document is digitally signed it is ready to be sent to the trading partner. The Sending Party sends the document with the result of the digital signature process.

According to point seen in previous points, there is a need to define parameters to be used for:

- Digest Algorithm
- Padding Algorithm
- Digital Signature Algorithm
- Digital Certificate Type
- Filtering techniques.

5.2 *Digest Algorithm*

It is strongly recommends to use hash algorithms with a resulting length of more that 128 bits for a good degree of robustness in the signing process. Most widely used and implemented digest algorithms are SHA-1 and RIPEMD-160, both of them have a result of 160 bits-length.

5.3 *Padding Algorithm*

Padding is a key algorithm that helps on the robustness of the signature. Effectively, padding is used to provide additional countermeasures to hackers, because it provides extra security functionalities. Padding includes random data to the hash value and reorders some bit-streams. By doing so, it is even more complex (both from theoretical and implementation point of view) to break a signature (i.e. the computational effort required increases exponentially).

For instance, SHA1 + RSA algorithm is no longer secure if we don't use a padding technique.

Padding Algorithms recommended:

- PCKS#1 Family (different versions allowed)

- ISO9796-2 Schema 2

5.4 *Digital Signature Algorithm*

Even if there are some digital signatures algorithms available in the market: DSA, RSA, ECC, …, nearly all Trusted CAs provide X509v3 Digital Certificates based on RSA keys. It is recommended to use RSA Algorithm to digitally sign the document.

5.5 *Digital Certificate Type*

There are different kinds of Digital certificates. Even if EDIFACT Digital Certificates (A Digital Certificate with EDIFACT structure) and others exist, the cost of these Digital Certificates is very high and they are not widely implemented. The most common certificate type is X.509v3 and it is generated by most of Trusted CAs.

Digital Certificates types allowed:

- EDIFACT
- X.509v3

5.6 *Filtering Algorithm*

The result of a Digital Signature process using RSA is a binary string. The filtering mechanism will convert octets containing arbitrary bit patterns are converted to octets belonging to the character set which the underlying syntax is capable of supporting.

Filter techniques allowed:

- Hexadecimal
- UN/CEFACT EDA Filter
- UN/CEFACT EDC Filter

ISO9735 recommends using the EDC Filter because of the resulting expanding ratio. EDC filter result is compatible with UNOC character set. While a hexadecimal filter has a ratio of 1 to 2, since each byte is represented by its hexadecimal value, the resulting expanding ratio of an EDC filter is from 7 to 8. For instance, a digital signature generated with a key of 1024 bits, gives a binary stream of 256 bytes with a hexadecimal filter and 152 bytes for the EDC Filter (40% less than the hexadecimal filter).

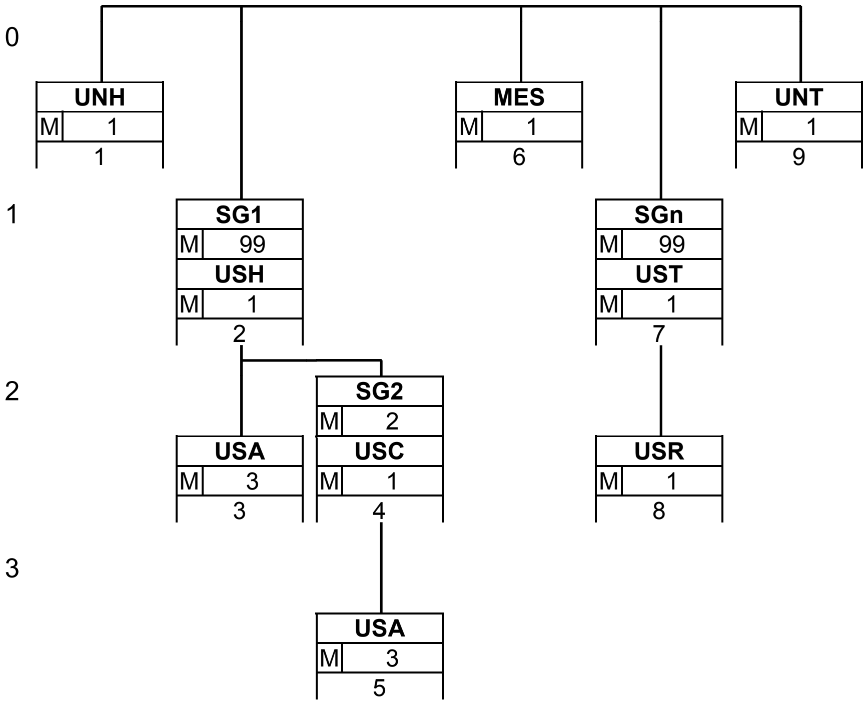
6 Attached Digital Signature

The objective of this chapter is to detail all technical parameters needed for the implementation of digital signature in EANCOM® D01B Syntax 4 messages.

6.1 *Message Structure Chart*

UNH	1	M	1	- Message header
SG1		M	99	- USH-USA-SG2
USH	2	M	1	- Security header
USA	3	M	3	- Security algorithm
SG2		M	2	- USC-USA
USC	4	M	1	- Certificate
USA	5	M	3	- Security algorithm
MES	6	M	1	- EANCOM message
SGn		M	99	- UST-USR
UST	7	M	1	- Security trailer
USR	8	M	1	- Security result
UNT	9	M	1	- Message trailer

6.2 *Branching Diagram*



6.3 *Segment Description*

UNH 1 - M 1 - Message header
This segment is used to head, identify and specify a message.

SG1 M99 -USH-USA-SG2

A group of segments identifying the security service and security mechanisms applied and containing the data necessary to carry out the validation calculations. This segment group shall specify the security service and algorithm(s) applied to the referenced EDIFACT structure. Each security header group shall be linked to a security trailer group, and additionally linked to the USY segment(s).
USH 2 - M 1 - Security header
A segment specifying a security service applied to the referenced EDIFACT structure.
USA 3 - M 3 - Security algorithm
This segment is used to identify a security algorithm, the technical usage made of it, and contains the technical parameters required in order to generate the hash value.

SG2 M2 -USC-USA

A group of segments containing the data necessary to validate the security methods applied.
USC 4 - M 1 - Certificate
This segment either contains information regarding the digital certificate used to sign the message. It also details the type of digital certificate used (EDIFACT or X.509v3).
USA 5 - M 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.
MES 6 - M 1 - EANCOM message
EANCOM D01B Message. This message shall follow Syntax 4 rules.

SGn M99 -UST-USR

A group of segments containing a link with security header segment group and the result of the security services applied to the message/package.
UST 7 - M 1 - Security trailer
A segment establishing a link between security header and security trailer segment group, and stating the number of security segments in these groups.
USR 8 - M 1 - Security result
A segment containing the result of the security functions applied to the message/package as specified in the linked security header group (as defined in Part 5 of ISO 9735). The security result in this segment shall be applied to the AUTACK message itself.
UNT 9 - M 1 - Message trailer

6.4 *Segment Layout*

This section describes each segment used in the EANCOM® Multiple Credit Advice 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.

Segment number: 1

UNH - M 1 - Message header

Function:

To head, identify and specify a message.

		EDIFACT	EAN	*	Description
0062	Message reference number	M an..14	**M**		Sender's unique message reference. Sequence number of messages in the interchange. DE 0062 in UNT will have the same value. Generated by the sender.
S009	MESSAGE IDENTIFIER	M	**M**		
0065	Message type	M an..6	**M**	*	XXXXXX = EDIFACT Message, Syntax 4
0052	Message version number	M an..3	**M**	*	D = Draft version/UN/EDIFACT Directory
0054	Message release number	M an..3	**M**	*	01B = Release 2001 - B
0051	Controlling agency, coded	M an..3	**M**	*	UN = UN/CEFACT
0057	Association assigned code	C an..6	**R**	*	XXX = EAN version control number (EAN 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 EAN.UCC.
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	**N**		
0073	First and last transfer	C a1	**N**		
S016	MESSAGE SUBSET IDENTIFICATION	C	**N**		
0115	Message subset identification	M an..14	**N**		
0116	Message subset version number	C an..3	**N**		
0118	Message subset release number	C an..3	**N**		
0051	Controlling agency, coded	C an..3	**N**		
S017	MESSAGE IMPLEMENTATION GUIDELINE IDENTIFICATION	C	**N**		
0121	Message implementation guideline identification	M an..14	**N**		
0122	Message implementation guideline version number	C an..3	**N**		
0124	Message implementation guideline release number	C an..3	**N**		
0051	Controlling agency, coded	C an..3	**N**		
S018	SCENARIO IDENTIFICATION	C	**N**		
0127	Scenario identification	M an..14	**N**		

Segment number: 1

		EDIFACT	EAN	*	Description
0128	Scenario version number	C an..3	**N**		
0130	Scenario release number	C an..3	**N**		
0051	Controlling agency, coded	C an..3	**N**		

Segment Notes:

This segment is used to head, identify and specify a message.
DE's 0065, 0052, 0054, and 0051: Indicate that the message is an UNSM AUTACK under the control of the United Nations Syntax 4.

Example:
UNH+MES00001+XXXXXX:D:01B:UN:EANXXX'
EAN to be replaced by GS1. EAN is detailed in the Segment since it is the official name of the code in D01B.

Segment number: 2

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

Function:

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

		EDIFACT	EAN	*	Description
0501	Security service, coded	M an..3	**M**	*	1 = Non-repudiation of origin
0534	Security reference number	M an..14	**M**		Unique reference number assigned by the security originator to the security header group, security trailer group and the USY segment (USH, DE 0534; UST, DE 0534 and USY, DE 0534).
0541	Scope of security application, coded	C an..3	**R**	*	Specification of the scope of application of the security service defined in the security header. 1 = Security header and message body 2 = From security header to security trailer
0503	Response type, coded	C an..3	**R**	*	1 = No acknowledgement required 2 = Acknowledgement required If an Acknowledgment message is detailed, the receiver of the message should send an AUTACK message after the validation of the Digital Signature. Regardless of this value if the Digital Process validation process fails, the AUTACK should also be sent.
0505	Filter function, coded	C an..3	**R**	*	2 = Hexadecimal filter 5 = UN/EDIFACT EDA filter 6 = UN/EDIFACT EDC filter Identification of the filtering function used to reversibly map any bit pattern to a restricted character set. The filter function describes how binary information (e.g., a digital signature) can be shown in a readable format. This is for example the case if the value "01111111 00111011" has no readable presentation and can be shown with the hexadecimal filter as "7F 3B".
0507	Original character set encoding, coded	C an..3	**R**	*	1 = ASCII 7 bit 2 = ASCII 8 bit 3 = Code page 850 (IBM PC Multinational) 4 = Code page 500 (EBCDIC Multinational No. 5) Identification of the character set in which the secured EDIFACT structure was encoded when security mechanisms were applied (i.e., when the digital signature was generated).
0509	Role of security provider, coded	C an..3	**R**	*	1 = Issuer
S500	SECURITY IDENTIFICATION DETAILS	C	**D**		
0577	Security party qualifier	M an..3	**M**	*	1 = Message sender
0538	Key name	C an..35	**N**		
0511	Security party identification	C an..512	**R**		GLN - Format n13

Segment number: 2

		EDIFACT	EAN	*	Description
0513	Security party code list qualifier	C an..3	**R**	*	2 = EAN
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**		
S500	SECURITY IDENTIFICATION DETAILS	C	**D**		
0577	Security party qualifier	M an..3	**M**	*	2 = Message receiver
0538	Key name	C an..35	**N**		
0511	Security party identification	C an..512	**R**		GLN - Format n13
0513	Security party code list qualifier	C an..3	**R**	*	2 = EAN
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**		
0520	Security sequence number	C an..35	**N**		
S501	SECURITY DATE AND TIME	C	**R**		
0517	Date and time qualifier	M an..3	**M**	*	1 = Security Timestamp 5 = EDIFACT structure generation date and time Date and time when the signature was generated. DE0517=1 only in case to have a third trusted party for Timestamping purposes.
0338	Event date	C n..8	**R**		Date of event, format is CCYYMDD.
0314	Event time	C an..15	**R**		Time of event, format is HHMMSS
0336	Time offset	C n4	**O**		UTC (Universal Co-ordinated Time) offset from event time. Format is HHMM. Shall be prefixed with '-' for negative offsets.

Segment Notes:

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

The parties involved in the security service (security elements originator and security elements recipient), may be identified in this segment, unless they are unambiguously identified by means of certificates (USC segment) when asymmetric algorithms are used.

Security identification details composite data element (S500) shall be used in USH segment asymmetric algorithms are used and when two certificates are present, in order to distinguish between the originator and the recipient certificates

Segment number: 2

In this latter case, the identification of the party in S500 (any of the data elements S500/0511, S500/0513, S500/0515, S500/0586) shall be the same as the identification of the party, qualified as "certificate owner" in one of the S500 present in the USC segment in segment group 2, and data element S500/0577 shall identify the function (originator or recipient) of the party involved.

Data element key name in security identification details composite data element (S500/0538) may be used to establish the key relationship between the sending and receiving

his key relationship may also be established by using the data element identification of the key of the algorithm parameter composite data element (S503/0554) in the USA segment of segment group 1.

S500/0538 in USH segment may be used if there is no need to convey a USA segment in segment group 1 (because the cryptographic mechanisms have been agreed previously between the partners).

Nevertheless, it is strongly recommended to use either S500/0538 in the USH segment, or S503/0554 with the appropriate qualifier in the USA segment, but not both of them, within the same security header group.

Example:
USH+5+1+2+1+6+2+1+1::8456789000007:2*2::8456789000014++5:20050607:161947:0100'
EAN to be replaced by GS1. EAN is detailed in the Segment since it is the official name of the code in D01B.

Segment number: 3

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

Function:

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

		EDIFACT	EAN	*	Description
S502	SECURITY ALGORITHM	M	**M**		
0523	Use of algorithm, coded	M an..3	**M**	*	1 = Owner hashing
0525	Cryptographic mode of operation, coded	C an..3	**N**		
0533	Mode of operation code list identifier	C an..3	**N**		
0527	Algorithm, coded	C an..3	**R**		14 = RIPEMD-160 16 = SHA1 Identification of the algorithm in order to generate the hash value. The algorithms above are recommended.
0529	Algorithm code list identifier	C an..3	**R**	*	1 = UN/CEFACT
0591	Padding mechanism, coded	C an..3	**N**		
0601	Padding mechanism code list identifier	C an..3	**N**		
S503	ALGORITHM PARAMETER	C	**N**		
0531	Algorithm parameter qualifier	M an..3	**N**		
0554	Algorithm parameter value	M an..512	**N**		

Segment Notes:

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

Example:
USA+1:::14:1'

Segment number: 4

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

Function:

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

		EDIFACT	EAN	*	Description
0536	Certificate reference	C an..35	**R**		Unique Certificate number assigned by a trusted party.
S500	SECURITY IDENTIFICATION DETAILS	C	**C**		
0577	Security party qualifier	M an..3	**M**		3 = Certificate owner Identification of the role of the security parties: signature key owner.
0538	Key name	C an..35	**N**		
0511	Security party identification	C an..512	**R**		For identification of parties it is recommended to use GLN - Format n13. If no GLN is available, Distinguised name(DN) of digital certificate will be detailed.
0513	Security party code list qualifier	C an..3	**R**	*	1 = ACH 2 = EAN 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**		
S500	SECURITY IDENTIFICATION DETAILS	C	**C**		
0577	Security party qualifier	M an..3	**M**	*	4 = Authenticating party Identification of the role of the security parties (trusted third party).
0538	Key name	C an..35	**N**		
0511	Security party identification	C an..512	**R**		For identification of parties it is recommended to use GLN - Format n13. If no GLN is available, Distinguised name(DN) of digital certificate will be detailed.
0513	Security party code list qualifier	C an..3	**R**	*	1 = ACH 2 = EAN 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	**M**	*	1 = EDIFACT version 4 3 = X.509

Segment number: 4

		EDIFACT	EAN	*	Description
					The certificate syntax and version shall be identified in data element 0545 of the USC segment. If the certificate used is not and EDIFACT certificate, such certificates may be conveyed in an EDIFACT package.
0505	Filter function, coded	C an..3	**N**		
0507	Original character set encoding, coded	C an..3	**N**		
0543	Certificate original character set repertoire, coded	C an..3	**N**		
0546	User authorisation level	C an..35	**N**		
S505	SERVICE CHARACTER FOR SIGNATURE	C	**N**		
0551	Service character for signature qualifier	M an..3	**M**		
0548	Service character for signature	M an..4	**N**		
S501	SECURITY DATE AND TIME	C	**N**		
0517	Date and time qualifier	M an..3	**N**		
0338	Event date	C n..8	**C**		
0314	Event time	C an..15	**C**		
0336	Time offset	C n4	**C**		
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 digital certificate used to sign the message. It also details the type of digital certificate used (EDIFACT or X.509v3).

Example :
USC+68EF+3::8456789000007:2*4::8456789000014:2+3'

Segment number: 5

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

Function:

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

		EDIFACT	EAN	*	Description
S502	SECURITY ALGORITHM	M	**M**		
0523	Use of algorithm, coded	M an..3	**M**	*	6 = Owner signing
0525	Cryptographic mode of operation, coded	C an..3	**R**	*	16 = DSMR Specification of the cryptographic mode of operation used for the algorithm. Note: The cryptographic mode of operation are the security functions authenticity, integrity and non-repudiation of origin. The digital signature includes all three security functions.
0533	Mode of operation code list identifier	C an..3	**R**	*	1 = UN/CEFACT
0527	Algorithm, coded	C an..3	**R**	*	10 = RSA
0529	Algorithm code list identifier	C an..3	**R**	*	1 = UN/CEFACT
0591	Padding mechanism, coded	C an..3	**C**		7 = ISO 9796 #2 padding 11 = PKCS #1 signature padding 16 = RSASA-PKCS-v1_5 17 = Encryption Block Formatting For ISO9796#2 padding, schema 2 has to be used.
0601	Padding mechanism code list identifier	C an..3	**R**	*	1 = UN/CEFACT
S503	ALGORITHM PARAMETER	C	**O**		
0531	Algorithm parameter qualifier	M an..3	**M**	*	14 = Modulus length
0554	Algorithm parameter value	M an..512	**M**		
S503	ALGORITHM PARAMETER	C	**O**		
0531	Algorithm parameter qualifier	M an..3	**M**	*	12 = Modulus
0554	Algorithm parameter value	M an..512	**M**		
S503	ALGORITHM PARAMETER	C	**O**		
0531	Algorithm parameter qualifier	M an..3	**M**	*	13 = Exponent
0554	Algorithm parameter value	M an..512	**M**		

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.

Example:

```
USA+6:16:1:10:1+14:1024+12:tÞïÏXC@{äcPÛõÈUùîsÜJïÛõÞmÖDØUJ@_@XUéÞ]l[□ âë{^ÍeèzãÉ}
gÍùAÄmEpV÷ÔÐBâÔ[ØßÝðKúÇÅÐíÈÑÎÝ\CýãëÐDvUYÂJòyÃ□ úP|kQBëWÖÓ^LßÈèÅÅnqmäÛhOÈÞÃ_]
DÜ_`Îÿì_zê`ÓjOgRÚ@BË+13:ðA@A'
```

Segment number: 7

SGn	- M	99 - UST-USR			
UST	- M	1 - Security trailer			

Function:

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

		EDIFACT	EAN	*	Description
0534	Security reference number	M an..14	**M**		Unique reference number assigned by the security originator to the security header group, security trailer group and the USY segment (USH, DE 0534; UST, DE 0534 and USY, DE 0534).
0588	Number of security segments	M n..10	**M**		The number of security segments in a security header/trailer group pair. Only the segment goups 1, 2 and 4 are counted. Each security header/trailer group pair shall contain its own count of the number of security segments within that group pair.

Segment Notes:

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

Example:
UST+1+6'

Segment number: 8

SGn	- M	99 -	UST-USR
USR	- M	1 -	Security result

Function:

To contain the result of the security mechanisms.

		EDIFACT	EAN	*	Description
S508	VALIDATION RESULT	M	**M**		
0563	Validation value, qualifier	M an..3	**M**	*	1 = Unique validation value
0560	Validation value	C an..512	**R**		Digital signature result corresponding to the security function specified. This value shall be filtered by an appropriate filter function.

Segment Notes:

A segment containing the result of the security functions applied to the message/package as specified in the linked security header group (as defined in Part 5 of ISO 9735). The security result in this segment shall be applied to the AUTACK message itself.

Example:
USR+1:ebãßÏÞÓñrGÁpÜúÑÄòóiJëÀDjôyQ\Ë}Ït}ÇçÉÂ^hñÕÜ}IjÈÍÃKÐÅÍJÉçàqã]F|dÁrôOÜÎ|KêÚ}
ãZxxÝk\gãoAïàVR`äÎÎxP\ëüÞrùRá^~\XÏeßXìâøPlúFñòwë_Á×ú\ãã}ý]øqØÄS_GvqS@ÔÏ'

Segment number: 9

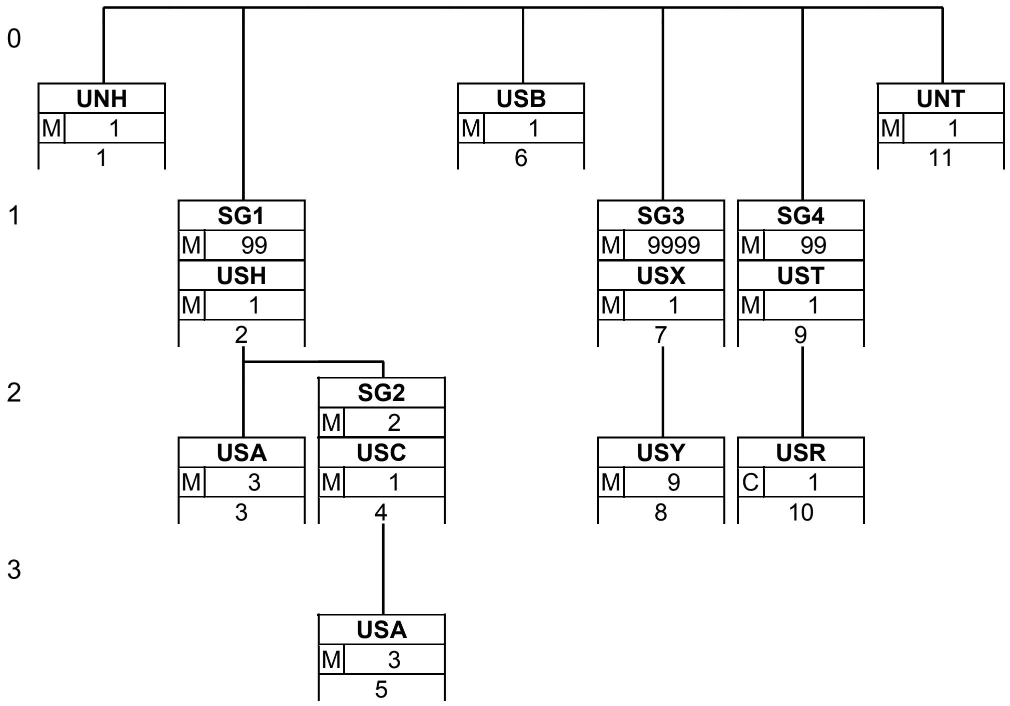
UNT	- M	1 - Message trailer			
Function: To end and check the completeness of a message.					
		EDIFACT	EAN	*	Description
0074	Number of segments in a message	M n..10	**M**		
0062	Message reference number	M an..14	**M**		
Segment Notes:					

7 AUTACK Message (Digital signature)

7.1 *Message Structure Chart*

UNH	1	M	1	- Message header
SG1		M	99	- USH-USA-SG2
USH	2	M	1	- Security header
USA	3	M	3	- Security algorithm
SG2		M	2	- USC-USA
USC	4	M	1	- Certificate
USA	5	M	3	- Security algorithm
USB	6	M	1	- Secured data identification
SG3		M	9999	- USX-USY
USX	7	M	1	- Security references
USY	8	M	9	- Security on references
SG4		M	99	- UST-USR
UST	9	M	1	- Security trailer
USR	10	C	1	- Security result
UNT	11	M	1	- Message trailer

7.2 *Branching Diagram*



7.3 *Segment Description*

UNH 1 - M 1 - Message header
This segment is used to head, identify and specify a message.

SG1 M 99 - USH-USA-SG2
A group of segments identifying the security service and security mechanisms applied and containing the data necessary to carry out the validation calculations.
This segment group shall specify the security service and algorithm(s) applied to the referenced EDIFACT structure. Each security header group shall be linked to a security trailer group, and additionally linked to the USY segment(s).

USH 2 - M 1 - Security header
A segment specifying a security service applied to the referenced EDIFACT structure.

USA 3 - M 3 - Security algorithm
This segment is used to identify a security algorithm, the technical usage made of it, and contains the technical parameters required in order to generate the hash value.

SG2 M 2 - USC-USA
A group of segments containing the data necessary to validate the security methods applied.

USC 4 - M 1 - Certificate
This segment either contains information regarding the digital certificate used to sign the message. It also details the type of digital certificate used (EDIFACT or X.509v3).

USA 5 - M 3 - Security algorithm
This segment is used to identify a security algorithm, the technical usage made of it, and contains the technical parameters required in order to generate the digital signature.

USB 6 - M 1 - Secured data identification
This segment shall contain identification of the interchange sender and interchange recipient.

SG3 M 9999 - USX-USY
This segment group shall be used to identify a party in the security process and to give security information for the referenced EDIFACT structure.

USX 7 - M 1 - Security references
This segment shall contain references to EDIFACT structures (i.e., interchanges, groups or messages) to which security services were applied.

USY 8 - M 9 - Security on references
This segment shall contain references to EDIFACT structures (i.e., interchanges, groups or messages) to which security services were applied.

SG4 M 99 - UST-USR
A group of segments containing a link with security header segment group and the result of the security services applied to the message/package.

UST 9 - M 1 - Security trailer
A segment establishing a link between security header and security trailer segment group, and stating the number of security segments in these groups.

USR 10 - C 1 - Security result
A segment containing the result of the security functions applied to the message/package as specified in the linked security header group (as defined in Part 5 of ISO 9735). The security result in this segment shall be applied to the AUTACK message itself.

UNT 11 - M 1 - Message trailer
A service segment ending a message, giving the total number of segments and the control reference number of the message.

7.4 *Segment Layout*

This section describes each segment used in the EANCOM® Multiple Credit Advice 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.

3. 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.

Segment number: 1

UNH - M 1 - Message header

Function:

To head, identify and specify a message.

		EDIFACT	EAN	*	Description
0062	Message reference number	M an..14	**M**		Sender's unique message reference. Sequence number of messages in the interchange. DE 0062 in UNT will have the same value. Generated by the sender.
S009	MESSAGE IDENTIFIER	M	**M**		
0065	Message type	M an..6	**M**	*	AUTACK = Secure authentication and acknowledgement message
0052	Message version number	M an..3	**M**	*	4 = Service message, version 4
0054	Message release number	M an..3	**M**	*	1 = First release
0051	Controlling agency, coded	M an..3	**M**	*	UN = UN/CEFACT
0057	Association assigned code	C an..6	**R**	*	EAN001 = EAN version control number (EAN 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 EAN.UCC.
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	**N**		
0073	First and last transfer	C a1	**N**		
S016	MESSAGE SUBSET IDENTIFICATION	C	**N**		
0115	Message subset identification	M an..14	**N**		
0116	Message subset version number	C an..3	**N**		
0118	Message subset release number	C an..3	**N**		
0051	Controlling agency, coded	C an..3	**N**		
S017	MESSAGE IMPLEMENTATION GUIDELINE IDENTIFICATION	C	**N**		
0121	Message implementation guideline identification	M an..14	**N**		
0122	Message implementation guideline version number	C an..3	**N**		
0124	Message implementation guideline release number	C an..3	**N**		
0051	Controlling agency, coded	C an..3	**N**		
			N		

Segment number: 1

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

Segment Notes:

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

Example:
UNH+AUT00001+AUTACK:4:1:UN:EAN001'
EAN to be replaced by GS1. EAN is detailed in the Segment since it is the official name of the code in D01B.

Segment number: 2

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

Function:

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

		EDIFACT	EAN	*	Description
0501	Security service, coded	M an..3	**M**	*	7 = Referenced EDIFACT structure non-repudiation of origin
0534	Security reference number	M an..14	**M**		Unique reference number assigned by the security originator to the security header group, security trailer group and the USY segment (USH, DE 0534; UST, DE 0534 and USY, DE 0534).
0541	Scope of security application, coded	C an..3	**R**	*	3 = Whole related message, package, group or interchange Specification of the scope of application of the security service defined in the security header.
0503	Response type, coded	C an..3	**C**	*	1 = No acknowledgement required
0505	Filter function, coded	C an..3	**R**	*	2 = Hexadecimal filter 5 = UN/EDIFACT EDA filter 6 = UN/EDIFACT EDC filter Identification of the filtering function used to reversibly map any bit pattern to a restricted character set. The filter function describes how binary information (e.g., a digital signature) can be shown in a readable format. This is for example the case if the value "01111111 00111011" has no readable presentation and can be shown with the hexadecimal filter as "7F 3B".
0507	Original character set encoding, coded	C an..3	**R**	*	1 = ASCII 7 bit 2 = ASCII 8 bit 3 = Code page 850 (IBM PC Multinational) 4 = Code page 500 (EBCDIC Multinational No. 5) Identification of the character set in which the secured EDIFACT structure was encoded when security mechanisms were applied (i.e., when the digital signature was generated).
0509	Role of security provider, coded	C an..3	**C**	*	1 = Issuer
S500	SECURITY IDENTIFICATION DETAILS	C	**D**		
0577	Security party qualifier	M an..3	**M**	*	1 = Message sender
0538	Key name	C an..35	**N**		
0511	Security party identification	C an..512	**R**		GLN - Format n13
0513	Security party code list qualifier	C an..3	**R**	*	2 = EAN
0515	Security party code list responsible agency, coded	C an..3	**N**		
			N		

Segment number: 2

		EDIFACT	EAN	*	Description
0586	Security party name	C an..35			
0586	Security party name	C an..35	**N**		
0586	Security party name	C an..35	**N**		
S500	SECURITY IDENTIFICATION DETAILS	C	**D**		
0577	Security party qualifier	M an..3	**M**	*	2 = Message receiver
0538	Key name	C an..35	**N**		
0511	Security party identification	C an..512	**R**		GLN - Format n13
0513	Security party code list qualifier	C an..3	**R**	*	2 = EAN
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**		
0520	Security sequence number	C an..35	**N**		
S501	SECURITY DATE AND TIME	C	**R**		
0517	Date and time qualifier	M an..3	**M**	*	1 = Security Timestamp 5 = EDIFACT structure generation date and time Date and time when the signature was generated. DE0517=1 only in case to have a third trusted party for Timestamping purposes.
0338	Event date	C n..8	**R**		Date of event, format is CCYYMDD.
0314	Event time	C an..15	**R**		Time of event, format is HHMMSS
0336	Time offset	C n4	**O**		UTC (Universal Co-ordinated Time) offset from event time. Format is HHMM. Shall be prefixed with '-' for negative offsets.

Segment Notes:

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

The parties involved in the security service (security elements originator and security elements recipient), may be identified in this segment, unless they are unambiguously identified by means of certificates (USC segment) when asymmetric algorithms are used.

Security identification details composite data element (S500) shall be used in USH segment asymmetric algorithms are used and when two certificates are present, in order to distinguish between the originator and the recipient certificates

In this latter case, the identification of the party in S500 (any of the data elements S500/0511, S500/0513, S500/0515, S500/0586) shall be the same as the identification of the party, qualified as "certificate owner" in one of the S500 present in the USC segment in segment group 2, and data element S500/0577 shall identify the function (originator or recipient) of the party involved.

Segment number: 2

Data element key name in security identification details composite data element (S500/0538) may be used to establish the key relationship between the sending and receiving

his key relationship may also be established by using the data element identification of the key of the algorithm parameter composite data element (S503/0554) in the USA segment of segment group 1.

S500/0538 in USH segment may be used if there is no need to convey a USA segment in segment group 1 (because the cryptographic mechanisms have been agreed previously between the partners).

Nevertheless, it is strongly recommended to use either S500/0538 in the USH segment, or S503/0554 with the appropriate qualifier in the USA segment, but not both of them, within the same security header group.

Example:

```
USH+7+1+3+1+6+2+1+1::8456789000007:2*2::8456789000014++5:20050607:161947:0100'
```

EAN to be replaced by GS1. EAN is detailed in the Segment since it is the official name of the code in D01B.

Segment number: 3

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

Function:

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

		EDIFACT	EAN	*	Description
S502	SECURITY ALGORITHM	M	**M**		
0523	Use of algorithm, coded	M an..3	**M**	*	1 = Owner hashing
0525	Cryptographic mode of operation, coded	C an..3	**N**		
0533	Mode of operation code list identifier	C an..3	**N**		
0527	Algorithm, coded	C an..3	**R**		14 = RIPEMD-160 16 = SHA1 Identification of the algorithm in order to generate the hash value. The algorithms above are recommended.
0529	Algorithm code list identifier	C an..3	**R**	*	1 = UN/CEFACT
0591	Padding mechanism, coded	C an..3	**N**		
0601	Padding mechanism code list identifier	C an..3	**N**		
S503	ALGORITHM PARAMETER	C	**N**		
0531	Algorithm parameter qualifier	M an..3	**N**		
0554	Algorithm parameter value	M an..512	**N**		

Segment Notes:

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

Example:
USA+1:::14:1'

Segment number: 4

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

Function:

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

		EDIFACT	EAN	*	Description
0536	Certificate reference	C an..35	**R**		Unique Certificate number assigned by a trusted party.
S500	SECURITY IDENTIFICATION DETAILS	C	**C**		
0577	Security party qualifier	M an..3	**M**		3 = Certificate owner Identification of the role of the security parties: signature key owner.
0538	Key name	C an..35	**N**		
0511	Security party identification	C an..512	**R**		For identification of parties it is recommended to use GLN - Format n13. If no GLN is available, Distinguised name(DN) of digital certificate will be detailed.
0513	Security party code list qualifier	C an..3	**R**	*	1 = ACH 2 = EAN 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**		
S500	SECURITY IDENTIFICATION DETAILS	C	**C**		
0577	Security party qualifier	M an..3	**M**	*	4 = Authenticating party Identification of the role of the security parties (trusted third party).
0538	Key name	C an..35	**N**		
0511	Security party identification	C an..512	**R**		For identification of parties it is recommended to use GLN - Format n13. If no GLN is available, Distinguised name(DN) of digital certificate will be detailed.
0513	Security party code list qualifier	C an..3	**R**	*	1 = ACH 2 = EAN 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	**M**	*	1 = EDIFACT version 4 3 = X.509

Segment number: 4

		EDIFACT	EAN	*	Description
					The certificate syntax and version shall be identified in data element 0545 of the USC segment. If the certificate used is not and EDIFACT certificate, such certificates may be conveyed in an EDIFACT package.
0505	Filter function, coded	C an..3	**N**		
0507	Original character set encoding, coded	C an..3	**N**		
0543	Certificate original character set repertoire, coded	C an..3	**N**		
0546	User authorisation level	C an..35	**N**		
S505	SERVICE CHARACTER FOR SIGNATURE	C	**N**		
0551	Service character for signature qualifier	M an..3	**M**		
0548	Service character for signature	M an..4	**N**		
S501	SECURITY DATE AND TIME	C	**N**		
0517	Date and time qualifier	M an..3	**N**		
0338	Event date	C n..8	**C**		
0314	Event time	C an..15	**C**		
0336	Time offset	C n4	**C**		
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 digital certificate used to sign the message. It also details the type of digital certificate used (EDIFACT or X.509v3).

Example :
USC+68EF+3::8456789000007:2*4::8456789000014:2+3'

Segment number: 5

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

Function:

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

		EDIFACT	EAN	*	Description
S502	SECURITY ALGORITHM	M	**M**		
0523	Use of algorithm, coded	M an..3	**M**	*	6 = Owner signing
0525	Cryptographic mode of operation, coded	C an..3	**R**	*	16 = DSMR Specification of the cryptographic mode of operation used for the algorithm. Note: The cryptographic mode of operation are the security functions authenticity, integrity and non-repudiation of origin. The digital signature includes all three security functions.
0533	Mode of operation code list identifier	C an..3	**R**	*	1 = UN/CEFACT
0527	Algorithm, coded	C an..3	**R**	*	10 = RSA
0529	Algorithm code list identifier	C an..3	**R**	*	1 = UN/CEFACT
0591	Padding mechanism, coded	C an..3	**C**		7 = ISO 9796 #2 padding 11 = PKCS #1 signature padding 16 = RSASA-PKCS-v1_5 17 = Encryption Block Formatting For ISO9796#2 padding, schema 2 has to be used.
0601	Padding mechanism code list identifier	C an..3	**R**	*	1 = UN/CEFACT
S503	ALGORITHM PARAMETER	C	**O**		
0531	Algorithm parameter qualifier	M an..3	**M**	*	14 = Modulus length
0554	Algorithm parameter value	M an..512	**M**		
S503	ALGORITHM PARAMETER	C	**O**		
0531	Algorithm parameter qualifier	M an..3	**M**	*	12 = Modulus
0554	Algorithm parameter value	M an..512	**M**		
S503	ALGORITHM PARAMETER	C	**O**		
0531	Algorithm parameter qualifier	M an..3	**M**	*	13 = Exponent
0554	Algorithm parameter value	M an..512	**M**		

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.

Example:

```
USA+6:16:1:10:1+14:1024+12:tÞïÏXC@{äcPÛõÈUùîsÜJïÛõÞmÖDØUJ@_@XUéÞ]l[□ âë{^ÍeèzãÉ}
gÍùAÄmEpV÷ÔÐBâÔ[ØßÝðKúÇÅÐíÈÑÎÝ\CýãëÐDvUYÂJòyÃ□ úP|kQBëWÖÓ^LßÈèÅÅnqmäÛhOÈÞÃ_]
DÜ_`Îÿì_zê`ÓjOgRÚ@BË+13:ðA@A'
```

Segment number: 6

USB - M 1 - Secured data identification					
Function: To contain details related to the AUTACK.					
		EDIFACT	EAN	*	Description
0503	Response type, coded	M an..3	**M**	*	1 = No acknowledgement required
S501	SECURITY DATE AND TIME	C	**O**		
0517	Date and time qualifier	M an..3	**M**	*	5 = EDIFACT structure generation date and time
0338	Event date	C n..8	**R**		Date of event, format is CCYYMMDD.
0314	Event time	C an..15	**R**		Time of event, format is HHMMSS
0336	Time offset	C n4	**O**		UTC (Universal Co-ordinated Time) offset from event time. Format is HHMM. Shall be prefixed with '-' for negative offsets.
S002	INTERCHANGE SENDER	M	**M**		
0004	Interchange sender identification	M an..35	**M**		GLN - Format n13
0007	Identification code qualifier	C an..4	**R**	*	14 = EAN (European Article Numbering Association)
0008	Interchange sender internal identification	C an..35	**N**		
0042	Interchange sender internal sub-identification	C an..35	**N**		
S003	INTERCHANGE RECIPIENT	M	**M**		
0010	Interchange recipient identification	M an..35	**M**		GLN - Format n13
0007	Identification code qualifier	C an..4	**R**	*	14 = EAN (European Article Numbering Association)
0014	Interchange recipient internal identification	C an..35	**N**		
0046	Interchange recipient internal sub-identification	C an..35	**N**		

Segment Notes:

This segment shall contain identification of the interchange sender and interchange recipient.
The interchange sender and interchange recipient in USB shall refer to the sender and the recipient of the interchange in which the AUTACK is present.

Example:
USB+1+5:20050606:100700+8456789000007:14+8456789000014:14'
EAN to be replaced by GS1. EAN is detailed in the Segment since it is the official name of the code in D01B.

Segment number: 7

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

Function:

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

		EDIFACT	EAN	*	Description
0020	Interchange control reference	M an..14	**M**		Unique reference number of interchange containing the data to which the security service was applied (UNB, DE 0020).
S002	INTERCHANGE SENDER	C	**C**		
0004	Interchange sender identification	M an..35	**M**		Identification of the party sending the interchange which contains the data to which security services were applied. It is recommended to use GLN - Format n13.
0007	Identification code qualifier	C an..4	**R**	*	14 = EAN (European Article Numbering Association)
0008	Interchange sender internal identification	C an..35	**N**		
0042	Interchange sender internal sub-identification	C an..35	**N**		
S003	INTERCHANGE RECIPIENT	C	**C**		
0010	Interchange recipient identification	M an..35	**M**		Identification of the party receiving the interchange which contains the data to which security services were applied. It is recommended to use GLN - Format n13.
0007	Identification code qualifier	C an..4	**R**	*	14 = EAN (European Article Numbering Association)
0014	Interchange recipient internal identification	C an..35	**N**		
0046	Interchange recipient internal sub-identification	C an..35	**N**		
0048	Group reference number	C an..14	**N**		
S006	APPLICATION SENDER IDENTIFICATION	C	**N**		
0040	Application sender identification	M an..35	**M**		
0007	Identification code qualifier	C an..4	**N**		
S007	APPLICATION RECIPIENT IDENTIFICATION	C	**N**		
0044	Application recipient identification	M an..35	**M**		
0007	Identification code qualifier	C an..4	**C**		
0062	Message reference number	C an..14	**D**		Reference number of a message (UNH to UNT) to which the security service was applied (UNH, DE 0062 of this message). Only applicable if the each document inside the interchange is signed, it is not necessary if the whole interchange is signed.

Segment number: 7

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

Segment Notes:

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

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

The USX segment we will use the following references of the received message with digital signature:
· DE 0020 Interchange reference number (UNB)
· DE 0062 Message reference number (UNH)

Example 1:
USX+INTERCHANGE1+++++MESSAGE003'

Example 2:
USX+INTERCHANGE1+++++MESSAGE003'

Segment number: 8

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

Function:

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

		EDIFACT	EAN	*	Description
0534	Security reference number	M an..14	**M**		Unique reference number assigned by the security originator to a pair of security header (USH, DE 0534) and security trailer groups (UST, DE 0534) as well as the value in this DE.
S508	VALIDATION RESULT	C	**R**		
0563	Validation value, qualifier	M an..3	**M**	*	1 = Unique validation value
0560	Validation value	C an..512	**R**		Security result corresponding to the security service specified, i.e., the value generated from the hash value of the data referenced in the USX segment with(Digital Signature Based) or without(Hash based) the private key of the signature originator specified in the USC segment. If necessary, this value shall be filtered by an appropriate filter function.
0571	Security error, coded	C an..3	**N**		

Segment Notes:

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

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

Segment number: 9

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

Function:

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

		EDIFACT	EAN	*	Description
0534	Security reference number	M an..14	**M**		Unique reference number assigned by the security originator to the security header group, security trailer group and the USY segment (USH, DE 0534; UST, DE 0534 and USY, DE 0534).
0588	Number of security segments	M n..10	**M**		The number of security segments in a security header/trailer group pair. Only the segment goups 1, 2 and 4 are counted. Each security header/trailer group pair shall contain its own count of the number of security segments within that group pair.

Segment Notes:

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

Example:
UST+1+6'

Segment number: 10

SG4	- M	99 -	UST-USR
USR	- C	1 -	Security result

Function:

To contain the result of the security mechanisms.

		EDIFACT	EAN	*	Description
S508	VALIDATION RESULT	M	**M**		
0563	Validation value, qualifier	M an..3	**M**	*	1 = Unique validation value
0560	Validation value	C an..512	**R**		Digital signature result corresponding to the security function specified. This value shall be filtered by an appropiate filter function.

Segment Notes:

A segment containing the result of the security functions applied to the message/package as specified in the linked security header group (as defined in Part 5 of ISO 9735). The security result in this segment shall be applied to the AUTACK message itself.

This segment is used if the AUTACK message itself is signed.

Example:

```
USR+1:ebãßÏÞÓñrGÁpÜúÑÄòóiJëÀDjôyQ\Ë}Ït}ÇçÉÂ^hñÕÜ}IjÈÍÃKÐÅÍJÉçàqã]F|dÁrôOÜÎ|KêÚ}
ãZxxÝk\gãoAïàVR`äÎÎxP\ëüÞrùRá^~\XÏeßXìâøPlúFñòwë_Á×ú\ãã}ý]øqØÄS_GvqS@ÔÏ'
```

Segment number: 11

UNT	- M	1 - Message trailer			
Function: To end and check the completeness of a message.					
		EDIFACT	EAN	*	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.

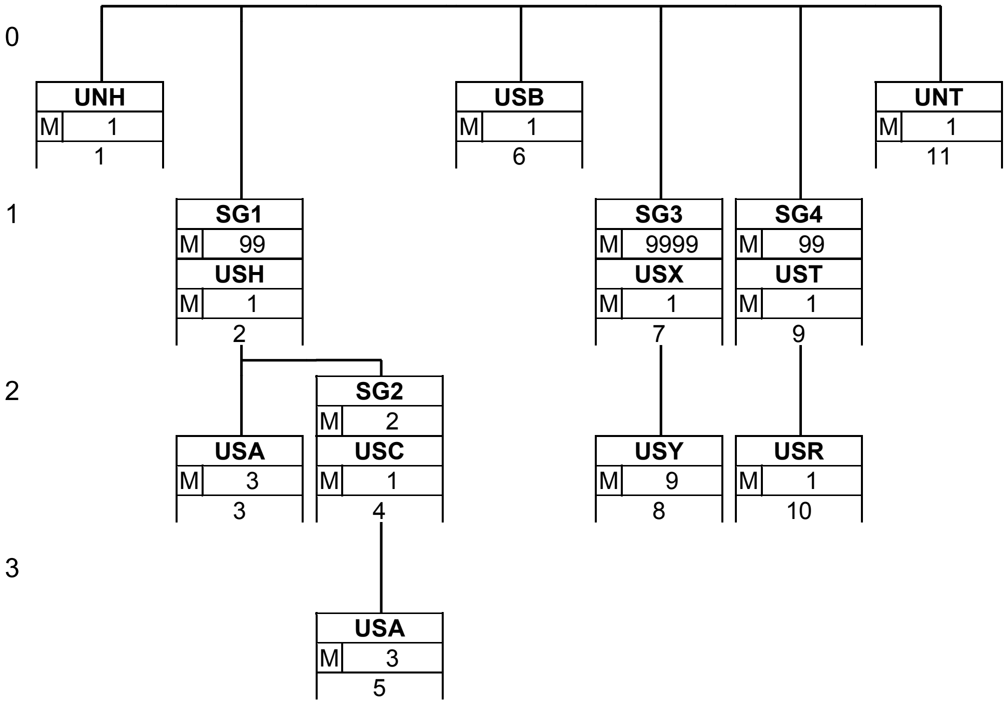
Example:
UNT+11+AUT00001'

8 AUTACK Message (Response)

8.1 *Message Structure Chart*

UNH	1	M	1	- Message header
SG1		M	99	- USH-USA-SG2
USH	2	M	1	- Security header
USA	3	M	3	- Security algorithm
SG2		M	2	- USC-USA
USC	4	M	1	- Certificate
USA	5	M	3	- Security algorithm
USB	6	M	1	- Secured data identification
SG3		M	9999	- USX-USY
USX	7	M	1	- Security references
USY	8	M	9	- Security on references
SG4		M	99	- UST-USR
UST	9	M	1	- Security trailer
USR	10	M	1	- Security result
UNT	11	M	1	- Message trailer

8.2 *Branching Diagram*



8.3 *Segment Description*

UNH 1 - M 1 - Message header
This segment is used to head, identify and specify a message.

SG1 M99 -USH-USA-SG2

A group of segments identifying the security service and security mechanisms applied and containing the data necessary to carry out the validation calculations. This segment group shall specify the security service and algorithm(s) applied to the referenced EDIFACT structure. Each security header group shall be linked to a security trailer group, and additionally linked to the USY segment(s).
USH 2 - M 1 - Security header
A segment specifying a security service applied to the referenced EDIFACT structure.
USA 3 - M 3 - Security algorithm
This segment is used to identify a security algorithm, the technical usage made of it, and contains the technical parameters required in order to generate the hash value.

SG2 M2 -USC-USA

A group of segments containing the data necessary to validate the security methods applied.
USC 4 - M 1 - Certificate
This segment either contains information regarding the digital certificate used to sign the message. It also details the type of digital certificate used (EDIFACT or X.509v3).
USA 5 - M 3 - Security algorithm
This segment is used to identify a security algorithm, the technical usage made of it, and contains the technical parameters required in order to generate the digital signature.
USB 6 - M 1 - Secured data identification
This segment shall contain identification of the interchange sender and interchange recipient.

SG3 M9999 -USX-USY

This segment group shall be used to identify a party in the security process and to give security information for the referenced EDIFACT structure.
USX 7 - M 1 - Security references
This segment shall contain references to EDIFACT structures (i.e., interchanges, groups or messages) to which security services were applied.
USY 8 - M 9 - Security on references
This segment shall contain references to EDIFACT structures (i.e., interchanges, groups or messages) to which security services were applied.

SG4 M99 -UST-USR

A group of segments containing a link with security header segment group and the result of the security services applied to the message/package.
UST 9 - M 1 - Security trailer
A segment establishing a link between security header and security trailer segment group, and stating the number of security segments in these groups.

USR 10 - M 1 - Security result
A segment containing the result of the security functions applied to the message/package as specified in the linked security header group (as defined in Part 5 of ISO 9735). The security result in this segment shall be applied to the AUTACK message itself.

UNT 11 - M 1 - Message trailer
A service segment ending a message, giving the total number of segments and the control reference number of the message.

8.4 *Segment Layout*

This section describes each segment used in the EANCOM® Multiple Credit Advice 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.

4. 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.

Segment number: 1

UNH	- M	1 - Message header			
Function: To head, identify and specify a message.					
		EDIFACT	EAN	*	Description
0062	Message reference number	M an..14	**M**		Sender's unique message reference. Sequence number of messages in the interchange. DE 0062 in UNT will have the same value. Generated by the sender.
S009	MESSAGE IDENTIFIER	M	**M**		
0065	Message type	M an..6	**M**	*	AUTACK = Secure authentication and acknowledgement message
0052	Message version number	M an..3	**M**	*	4 = Service message, version 4
0054	Message release number	M an..3	**M**	*	1 = First release
0051	Controlling agency, coded	M an..3	**M**	*	UN = UN/CEFACT
0057	Association assigned code	C an..6	**R**	*	EAN001 = EAN version control number (EAN 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 EAN.UCC.
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	**N**		
0073	First and last transfer	C a1	**N**		
S016	MESSAGE SUBSET IDENTIFICATION	C	**N**		
0115	Message subset identification	M an..14	**N**		
0116	Message subset version number	C an..3	**N**		
0118	Message subset release number	C an..3	**N**		
0051	Controlling agency, coded	C an..3	**N**		
S017	MESSAGE IMPLEMENTATION GUIDELINE IDENTIFICATION	C	**N**		
0121	Message implementation guideline identification	M an..14	**N**		
0122	Message implementation guideline version number	C an..3	**N**		
0124	Message implementation guideline release number	C an..3	**N**		
0051	Controlling agency, coded	C an..3	**N**		
			N		

Segment number: 1

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

Segment Notes:

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

Example:
UNH+AUT00001+AUTACK:4:1:UN:EAN001'
EAN to be replaced by GS1. EAN is detailed in the Segment since it is the official name of the code in D01B.

Segment number: 2

SG1 - M 99 - USH-USA-SG2

USH - M 1 - Security header

Function:

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

		EDIFACT	EAN	*	Description
0501	Security service, coded	M an..3	**M**	*	5 = Non-repudiation of receipt
0534	Security reference number	M an..14	**M**		Unique reference number assigned by the security originator to the security header group, security trailer group and the USY segment (USH, DE 0534; UST, DE 0534 and USY, DE 0534).
0541	Scope of security application, coded	C an..3	**R**	*	Specification of the scope of application of the security service defined in the security header. 1 = Security header and message body 2 = From security header to security trailer
0503	Response type, coded	C an..3	**C**	*	1 = No acknowledgement required
0505	Filter function, coded	C an..3	**R**	*	2 = Hexadecimal filter 5 = UN/EDIFACT EDA filter 6 = UN/EDIFACT EDC filter Identification of the filtering function used to reversibly map any bit pattern to a restricted character set. The filter function describes how binary information (e.g., a digital signature) can be shown in a readable format. This is for example the case if the value "01111111 00111011" has no readable presentation and can be shown with the hexadecimal filter as "7F 3B".
0507	Original character set encoding, coded	C an..3	**R**	*	1 = ASCII 7 bit 2 = ASCII 8 bit 3 = Code page 850 (IBM PC Multinational) 4 = Code page 500 (EBCDIC Multinational No. 5) Identification of the character set in which the secured EDIFACT structure was encoded when security mechanisms were applied (i.e., when the digital signature was generated).
0509	Role of security provider, coded	C an..3	**R**	*	1 = Issuer
S500	SECURITY IDENTIFICATION DETAILS	C	**D**		
0577	Security party qualifier	M an..3	**M**	*	1 = Message sender
0538	Key name	C an..35	**N**		
0511	Security party identification	C an..512	**R**		GLN - Format n13
0513	Security party code list qualifier	C an..3	**R**	*	2 = EAN
0515	Security party code list responsible agency, coded	C an..3	**N**		
0586	Security party name	C an..35	**N**		

Segment number: 2

		EDIFACT	EAN	*	Description
0586	Security party name	C an..35	**N**		
0586	Security party name	C an..35	**N**		
S500	SECURITY IDENTIFICATION DETAILS	C	**D**		
0577	Security party qualifier	M an..3	**M**	*	2 = Message receiver
0538	Key name	C an..35	**N**		
0511	Security party identification	C an..512	**R**		GLN - Format n13
0513	Security party code list qualifier	C an..3	**R**	*	2 = EAN
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**		
0520	Security sequence number	C an..35	**N**		
S501	SECURITY DATE AND TIME	C	**R**		
0517	Date and time qualifier	M an..3	**M**	*	1 = Security Timestamp 5 = EDIFACT structure generation date and time Date and time when the signature was generated. DE0517=1 only in case to have a third trusted party for Timestamping purposes.
0338	Event date	C n..8	**R**		Date of event, format is CCYYMDD.
0314	Event time	C an..15	**R**		Time of event, format is HHMMSS
0336	Time offset	C n4	**O**		UTC (Universal Co-ordinated Time) offset from event time. Format is HHMM. Shall be prefixed with '-' for negative offsets.

Segment Notes:

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

The parties involved in the security service (security elements originator and security elements recipient), may be identified in this segment, unless they are unambiguously identified by means of certificates (USC segment) when asymmetric algorithms are used.

Security identification details composite data element (S500) shall be used in USH segment asymmetric algorithms are used and when two certificates are present, in order to distinguish between the originator and the recipient certificates

In this latter case, the identification of the party in S500 (any of the data elements S500/0511, S500/0513, S500/0515, S500/0586) shall be the same as the identification of the party, qualified as "certificate owner" in one of the S500 present in the USC segment in segment group 2, and data element S500/0577 shall identify the function (originator or recipient) of the party involved.

Data element key name in security identification details composite data element (S500/0538) may be used to establish the key relationship between the sending and receiving

Segment number: 2

his key relationship may also be established by using the data element identification of the key of the algorithm parameter composite data element (S503/0554) in the USA segment of segment group 1.

S500/0538 in USH segment may be used if there is no need to convey a USA segment in segment group 1 (because the cryptographic mechanisms have been agreed previously between the partners).

Nevertheless, it is strongly recommended to use either S500/0538 in the USH segment, or S503/0554 with the appropriate qualifier in the USA segment, but not both of them, within the same security header group.

Example:
USH+5+1+2+1+6+2+1+1::8456789000007:2*2::8456789000014++5:20050607:161947:0100'
EAN to be replaced by GS1. EAN is detailed in the Segment since it is the official name of the code in D01B.

Segment number: 3

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

Function:

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

		EDIFACT	EAN	*	Description
S502	SECURITY ALGORITHM	M	**M**		
0523	Use of algorithm, coded	M an..3	**M**	*	1 = Owner hashing
0525	Cryptographic mode of operation, coded	C an..3	**N**		
0533	Mode of operation code list identifier	C an..3	**N**		
0527	Algorithm, coded	C an..3	**R**		14 = RIPEMD-160 16 = SHA1 Identification of the algorithm in order to generate the hash value. The algorithms above are recommended.
0529	Algorithm code list identifier	C an..3	**R**	*	1 = UN/CEFACT
0591	Padding mechanism, coded	C an..3	**N**		
0601	Padding mechanism code list identifier	C an..3	**N**		
S503	ALGORITHM PARAMETER	C	**N**		
0531	Algorithm parameter qualifier	M an..3	**N**		
0554	Algorithm parameter value	M an..512	**N**		

Segment Notes:

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

Example:
USA+1:::14:1'

Segment number: 4

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

Function:

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

		EDIFACT	EAN	*	Description
0536	Certificate reference	C an..35	**R**		Unique Certificate number assigned by a trusted party.
S500	SECURITY IDENTIFICATION DETAILS	C	**C**		
0577	Security party qualifier	M an..3	**M**		3 = Certificate owner Identification of the role of the security parties: signature key owner.
0538	Key name	C an..35	**N**		
0511	Security party identification	C an..512	**R**		For identification of parties it is recommended to use GLN - Format n13. If no GLN is available, Distinguised name(DN) of digital certificate will be detailed.
0513	Security party code list qualifier	C an..3	**R**	*	1 = ACH 2 = EAN 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**		
S500	SECURITY IDENTIFICATION DETAILS	C	**C**		
0577	Security party qualifier	M an..3	**M**	*	4 = Authenticating party Identification of the role of the security parties (trusted third party).
0538	Key name	C an..35	**N**		
0511	Security party identification	C an..512	**R**		For identification of parties it is recommended to use GLN - Format n13. If no GLN is available, Distinguised name(DN) of digital certificate will be detailed.
0513	Security party code list qualifier	C an..3	**R**	*	1 = ACH 2 = EAN 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	**M**	*	1 = EDIFACT version 4 3 = X.509

Segment number: 4

		EDIFACT	EAN	*	Description
					The certificate syntax and version shall be identified in data element 0545 of the USC segment. If the certificate used is not and EDIFACT certificate, such certificates may be conveyed in an EDIFACT package.
0505	Filter function, coded	C an..3	**N**		
0507	Original character set encoding, coded	C an..3	**N**		
0543	Certificate original character set repertoire, coded	C an..3	**N**		
0546	User authorisation level	C an..35	**N**		
S505	SERVICE CHARACTER FOR SIGNATURE	C	**N**		
0551	Service character for signature qualifier	M an..3	**M**		
0548	Service character for signature	M an..4	**N**		
S501	SECURITY DATE AND TIME	C	**N**		
0517	Date and time qualifier	M an..3	**N**		
0338	Event date	C n..8	**C**		
0314	Event time	C an..15	**C**		
0336	Time offset	C n4	**C**		
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 digital certificate used to sign the message. It also details the type of digital certificate used (EDIFACT or X.509v3).

Example :
USC+68EF+3::8456789000007:2*4::8456789000014:2+3'

Segment number: 5

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

Function:

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

		EDIFACT	EAN	*	Description
S502	SECURITY ALGORITHM	M	**M**		
0523	Use of algorithm, coded	M an..3	**M**	*	6 = Owner signing
0525	Cryptographic mode of operation, coded	C an..3	**R**	*	16 = DSMR Specification of the cryptographic mode of operation used for the algorithm. Note: The cryptographic mode of operation are the security functions authenticity, integrity and non-repudiation of origin. The digital signature includes all three security functions.
0533	Mode of operation code list identifier	C an..3	**R**	*	1 = UN/CEFACT
0527	Algorithm, coded	C an..3	**R**	*	10 = RSA
0529	Algorithm code list identifier	C an..3	**R**	*	1 = UN/CEFACT
0591	Padding mechanism, coded	C an..3	**C**		7 = ISO 9796 #2 padding 11 = PKCS #1 signature padding 16 = RSASA-PKCS-v1_5 17 = Encryption Block Formatting For ISO9796#2 padding, schema 2 has to be used.
0601	Padding mechanism code list identifier	C an..3	**R**	*	1 = UN/CEFACT
S503	ALGORITHM PARAMETER	C	**O**		
0531	Algorithm parameter qualifier	M an..3	**M**	*	14 = Modulus length
0554	Algorithm parameter value	M an..512	**M**		
S503	ALGORITHM PARAMETER	C	**O**		
0531	Algorithm parameter qualifier	M an..3	**M**	*	12 = Modulus
0554	Algorithm parameter value	M an..512	**M**		
S503	ALGORITHM PARAMETER	C	**O**		
0531	Algorithm parameter qualifier	M an..3	**M**	*	13 = Exponent
0554	Algorithm parameter value	M an..512	**M**		

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.

Example:

```
USA+6:16:1:10:1+14:1024+12:tÞïÏXC@{äcPÛõÈUùîsÜJïÛõÞmÖDØUJ@_@XUéÞ]I[□ âë{^ÍeèzãÉ}
gÍùAÄmEpV÷ÔÐBâÔ[ØßÝðKúÇÅÐíÈÑÎÝ\CýãëÐDvUYÂJòyÃ□ úP|kQBëWÖÓ^LßÈèÅÅnqmäÛhOÈÞÃ_]
DÜ_`Îÿì_zê`ÓjOgRÚ@BË+13:ðA@A'
```

Segment number: 6

USB - M 1 - Secured data identification					
Function: To contain details related to the AUTACK.					
		EDIFACT	EAN	*	Description
0503	Response type, coded	M an..3	**M**	*	1 = No acknowledgement required
S501	SECURITY DATE AND TIME	C	**O**		
0517	Date and time qualifier	M an..3	**M**	*	5 = EDIFACT structure generation date and time
0338	Event date	C n..8	**R**		Date of event, format is CCYYMMDD.
0314	Event time	C an..15	**R**		Time of event, format is HHMMSS
0336	Time offset	C n4	**O**		UTC (Universal Co-ordinated Time) offset from event time. Format is HHMM. Shall be prefixed with '-' for negative offsets.
S002	INTERCHANGE SENDER	M	**M**		
0004	Interchange sender identification	M an..35	**M**		GLN - Format n13
0007	Identification code qualifier	C an..4	**R**	*	14 = EAN (European Article Numbering Association)
0008	Interchange sender internal identification	C an..35	**N**		
0042	Interchange sender internal sub-identification	C an..35	**N**		
S003	INTERCHANGE RECIPIENT	M	**M**		
0010	Interchange recipient identification	M an..35	**M**		GLN - Format n13
0007	Identification code qualifier	C an..4	**R**	*	14 = EAN (European Article Numbering Association)
0014	Interchange recipient internal identification	C an..35	**N**		
0046	Interchange recipient internal sub-identification	C an..35	**N**		

Segment Notes:

This segment shall contain identification of the interchange sender and interchange recipient.
The interchange sender and interchange recipient in USB shall refer to the sender and the recipient of the interchange in which the AUTACK is present.

Example:
USB+1+5:20050606:100700+8456789000007:14+8456789000014:14'
EAN to be replaced by GS1. EAN is detailed in the Segment since it is the official name of the code in D01B.

Segment number: 7

SG3 - M 9999 - USX-USY

USX - M 1 - Security references

Function:

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

		EDIFACT	EAN	*	Description
0020	Interchange control reference	M an..14	**M**		Unique reference number of interchange containing the data to which the security service was applied (UNB, DE 0020).
S002	INTERCHANGE SENDER	C	**N**		
0004	Interchange sender identification	M an..35	**N**		
0007	Identification code qualifier	C an..4	**N**		
0008	Interchange sender internal identification	C an..35	**N**		
0042	Interchange sender internal sub-identification	C an..35	**N**		
S003	INTERCHANGE RECIPIENT	C	**N**		
0010	Interchange recipient identification	M an..35	**N**		
0007	Identification code qualifier	C an..4	**N**		
0014	Interchange recipient internal identification	C an..35	**N**		
0046	Interchange recipient internal sub-identification	C an..35	**N**		
0048	Group reference number	C an..14	**N**		
S006	APPLICATION SENDER IDENTIFICATION	C	**N**		
0040	Application sender identification	M an..35	**M**		
0007	Identification code qualifier	C an..4	**N**		
S007	APPLICATION RECIPIENT IDENTIFICATION	C	**N**		
0044	Application recipient identification	M an..35	**M**		
0007	Identification code qualifier	C an..4	**C**		
0062	Message reference number	C an..14	**R**		Reference number of a message (UNH to UNT) to which the security service was applied (UNH, DE 0062 of this message).
S009	MESSAGE IDENTIFIER	C	**N**		
0065	Message type	M an..6	**N**		
0052	Message version number	M an..3	**N**		
0054	Message release number	M an..3	**N**		
0051	Controlling agency, coded	M an..3	**N**		
0057	Association assigned code	C an..6	**N**		

Segment number: 7

		EDIFACT	EAN	*	Description
0110	Code list directory version number	C an..6	**N**		
0113	Message type sub-function identification	C an..6	**N**		
0800	Package reference number	C an..35	**N**		
S501	SECURITY DATE AND TIME	C	**N**		
0517	Date and time qualifier	M an..3	**N**		
0338	Event date	C n..8	**N**		
0314	Event time	C an..15	**N**		
0336	Time offset	C n4	**N**		

Segment Notes:

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

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

The USX segment we will use the following references of the received message with digital signature:
· DE 0020 Interchange reference number (UNB)
· DE 0062 Message reference number (UNH)

Example:
USX+INTERCHANGE1+++++MESSAGE003'

Segment number: 8

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

Function:

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

		EDIFACT	EAN	*	Description
0534	Security reference number	M an..14	**M**		
S508	VALIDATION RESULT	C	**N**		
0563	Validation value, qualifier	M an..3	**N**		
0560	Validation value	C an..512	**N**		
0571	Security error, coded	C an..3	**D**	*	1 = Wrong authenticator 2 = Wrong certificate 3 = Certification path 4 = Algorithm not supported 5 = Hashing method not supported 6 = Protocol error 7 = Security expected but not present 8 = Security parameters do not match those expected DE0571 only to be used if the validation of the digital signature of the message received fails.

Segment Notes:

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

Example:
USY+ME0001' -> Correct Message
USY+ME0001++1' -> Problems validating the digital signature

Segment number: 9

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

Function:

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

		EDIFACT	EAN	*	Description
0534	Security reference number	M an..14	**M**		Unique reference number assigned by the security originator to the security header group, security trailer group and the USY segment (USH, DE 0534; UST, DE 0534 and USY, DE 0534).
0588	Number of security segments	M n..10	**M**		The number of security segments in a security header/trailer group pair. Only the segment goups 1, 2 and 4 are counted. Each security header/trailer group pair shall contain its own count of the number of security segments within that group pair.

Segment Notes:

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

Example:
UST+1+6'

Segment number: 10

SG4	- M	99 -	UST-USR
USR	- M	1 -	Security result

Function:

To contain the result of the security mechanisms.

		EDIFACT	EAN	*	Description
S508	VALIDATION RESULT	M	**M**		
0563	Validation value, qualifier	M an..3	**M**	*	1 = Unique validation value
0560	Validation value	C an..512	**R**		Digital signature result corresponding to the security function specified. This value shall be filtered by an appropiate filter function.

Segment Notes:

A segment containing the result of the security functions applied to the message/package as specified in the linked security header group (as defined in Part 5 of ISO 9735). The security result in this segment shall be applied to the AUTACK message itself.

Example:
USR+1:ebãßÏÞÓñrGÁpÜúÑÄòóiJëÀDjôyQ\Ë}Ït}ÇçÉÂ^hñÕÜ}IjÈÍÃKÐÅÍJÉçàqã]F|dÁrôOÜÎ|KêÚ}
ãZxxÝk\gãoAïàVR`äÎÎxP\ëüÞrùRá^~\XÏeßXìâøP|úFñòwë_Á×ú\ãã}ý]øqØÄS_GvqS@ÔÏ'

Segment number: 11

UNT	- M	1 - Message trailer			
Function: To end and check the completeness of a message.					
		EDIFACT	EAN	*	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+11+AUT00001'

9 X.509v3 Digital Certificate conveyed in a EDIFACT interchange

9.1 *Segment Layout*

This section describes each segment used in the EANCOM® Multiple Credit Advice 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.

5. 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.

Segment number: 6

UNO - M 1 - Object header

Function:

To head, identify and specify an object.

		EDIFACT	EAN	*	Description
0800	Package reference number	M an..35	**M**		Unique pacakage reference number assigned by the sender
S020	REFERENCE IDENTIFICATION	M	**M**		
0813	Reference qualifier	M an..3	**M**	*	1 = Object identification number
0802	Reference identification number	M an..35	**M**		Reference number to identify a group which relates to the object.
S021	OBJECT TYPE IDENTIFICATION	M	**M**		
0805	Object type qualifier	M an..3	**M**	*	48 = Filter type
0809	Object type attribute identification	C an..256	**R**	*	EDA = UN/EDIFACT EDA filter EDC = UN/EDIFACT EDC filter HEX = Hexadecimal filter
0808	Object type attribute	C an..256	**N**		
0051	Controlling agency, coded	C an..3	**N**		
S021	OBJECT TYPE IDENTIFICATION	M	**M**		
0805	Object type qualifier	M an..3	**M**	*	62 = Certificate format
0809	Object type attribute identification	C an..256	**R**	*	PCKS7 = PKCS#7 format including the whole certification path if wished.
0808	Object type attribute	C an..256	**N**		
0051	Controlling agency, coded	C an..3	**N**		
S022	STATUS OF THE OBJECT	M	**M**		
0810	Length of object in octets of bits	M n..18	**M**		Length of the object attached in bytes
0814	Number of segments before object	C n..3	**N**		
0070	Sequence of transfers	C n..2	**N**		
0073	First and last transfer	C a1	**N**		
S302	DIALOGUE REFERENCE	C	**N**		
0300	Initiator control reference	M an..35	**N**		
0303	Initiator reference identification	C an..35	**N**		
0051	Controlling agency, coded	C an..3	**N**		
0304	Responder control reference	C an..35	**N**		
S301	STATUS OF TRANSFER - INTERACTIVE	C	**N**		
0320	Sender sequence number	C n..6	**N**		
0323	Transfer position, coded	C a1	**N**		
0325	Duplicate Indicator	C a1	**N**		

Segment number: 6

		EDIFACT	EAN	*	Description
S300	DATE AND/OR TIME OF INITIATION	C	**N**		
0338	Event date	C n..8	**N**		
0314	Event time	C an..15	**N**		
0336	Time offset	C n4	**N**		
0035	Test indicator	C n1	**N**		

Segment Notes:

This segment is udes to head, identify and specify an object.

The digital certificate will be attached using PKCS#7 format because it allows to include more than one digital certificate (User Certificate and the Certification Chain). This file will be filtered using EDC or Hexadecimal filter. Once the file is filtered, the total number of bytes of the object to be attached will be obtained and detailed in DE0810.

Example:
UNO+OB000001+1:CER123+46:EDC*62:PKCS7+1238'

Segment number: 7

UNP	- M	1 - Object trailer			
Function: To end and check the completeness of an object.					
		EDIFACT	EAN	*	Description
0810	Length of object in octets of bits	M n..18	**M**		This Data Element shall be identical to DE0810 of UNO segment.
0800	Package reference number	M an..35	**M**		This Data Element shall be identical to DE0800 of UNO segment.
Segment Notes: To end and check the completness of an object. Example: UNP+1238+OB000001'					

10 How to implement the digital Signature in 10 steps

This part of the document is a guideline for Software providers to implement the digital signature as it is detailed in this implementation guideline in ther e-commerce/B2B Softwares.

Process has been divided into three parts:

- Generation/validation of digital signature
- Digital Certificate Management
- Interoperability Test

	Done?	
Action	Yes	No
Generation/validation of digital signature		
Generate hash algorithms: SHA1 and RIPEMD-160		
Implement Padding algorithms: ISO9796-2 Schema 2 and PKCS#1 familiy		
Implement digital signature algorithm: RSA		
Filtering algorithms: EDC, Base64 and Hexadecimal		
Generate security header and tailer and include the digital signature in an EANCOM document		
Digital signature validation process		
Generation of AUTACK message		
Reception of AUTACK message		
Digital Certificate Management		
Digital Certificate Repository		
Include digital certificate in EDIFACT package: Segments UNO/UNP		
Obtain digital certificate from EDIFACT package: Segments UNO/UNP		
Interoperability Test		
Test with other Digital Signature softwares		

Appendice 1.- Bibliography

Electronic data interchange for administration, commerce and transport (EDIFACT)
Application level syntax rules
Joint ISO/TC 154 – UN/CEFACT Syntax Working Group (JSWG), ISO 9735-5 (01-04-1999)
Part 5: Security rules for batch EDI (authenticity, integrity and non-repudiation of origin)

Electronic data interchange for administration, commerce and transport (EDIFACT)
Application level syntax rules
Joint ISO/TC 154 – UN/CEFACT Syntax Working Group (JSWG), ISO 9735-6 (01-04-1999)
Part 6: Secure authentication and acknowledgement message (message type – AUTACK)

Electronic data interchange for administration, commerce and transport (EDIFACT)
Application level syntax rules
Joint ISO/TC 154 – UN/CEFACT Syntax Working Group (JSWG), ISO 9735-8 (01-04-1999)
Part 8: Associated data in EDI