UNITED
NATIONS

E

Economic and Social
Council

Distr.
RESTRICTED

TRADE/WP.4/R.1251/Rev.2
30 June 1997

ENGLISH ONLY

ECONOMIC COMMISSION FOR EUROPE

COMMITTEE FOR TRADE, INDUSTRY AND ENTERPRISE DEVELOPMENT

Centre for the Facilitation of Procedures
and Practices for Administration,
Commerce and Transport
(Item 3 of the provisional agenda of the
Meeting of Experts on Data Elements
and Automatic Data Interchange (GE.1)
(fifty-sixth session, 17-18 September 1997)

ELECTRONIC DATA INTERCHANGE FOR ADMINISTRATION, COMMERCE AND TRANSPORT (EDIFACT) - APPLICATION LEVEL SYNTAX RULES

Part 7
Security rules for batch EDI (confidentiality)

* * *

Submitted by the Syntax Development Group *

As requested during the March 1997 sessions of GE.1 and CEFACT, this document presents Part 7 of the revised EDIFACT syntax as prepared by the Syntax Development Group and will, upon approval, be submitted to ISO. It takes into account comments received on the previous version.

The Group of Experts is invited to: approve this document.

* The present document is reproduced in the form in which it was received by the secretariat.

ISO 9735-7

Release 2
1997-06-13

Electronic data interchange for administration, commerce and transport - (EDIFACT) - Application level syntax rules

Part 7:
Security rules for batch EDI (confidentiality)

Contents

		Page
Foreword		4
Introduction		5
1	**Scope**	**6**
2	**Conformance**	**6**
3	**Normative references**	**6**
4	**Definitions**	**6**
5	**Rules for batch EDI confidentiality**	**7**
ANNEX A: Syntax service directories		**15**
ANNEX B: Message protection example		**20**
ANNEX C: Processing example		**22**
ANNEX D: Confidentiality service and algorithms		**24**

Foreword

(To be amended as necessary, according to ISO procedures)

ISO (the International Organisation for Standardisation) is a world-wide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organisations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardisation.

Draft International Standards adopted by the technical committees are circulated to the member bodies for approval before their acceptance as International Standards by the ISO Council. They are approved in accordance with ISO procedures requiring at least 75% approval by the member bodies voting.

International Standard ISO 9735 Release 2 was prepared by the UN/ECE Trade Division (as UN/EDIFACT) and was adopted, under the "fast-track procedure" as an existing standard, by Technical Committee ISO TC 154, *Documents and data elements in administration; commerce and industry.*

ISO 9735 consists (currently) of the following parts, under the general title *Electronic data interchange for administration, commerce and transport (EDIFACT) - Application level syntax rules:*

ISO 9735-1	-	*Syntax rules common to all parts and the syntax service directories*
ISO 9735-2	-	*Syntax rules specific to batch EDI*
ISO 9735-3	-	*Syntax rules specific to interactive EDI*
ISO 9735-4	-	*Syntax and service report message for batch EDI (message type - CONTRL)*
ISO 9735-5	-	*Security rules for batch EDI (authenticity, integrity and non-repudiation of origin)*
ISO 9735-6	-	*Secure authentication and acknowledgement message (message type - AUTACK)*
ISO 9735-7	-	*Security rules for batch EDI (confidentiality)*
ISO 9735-8	-	*Associated data in EDI*
ISO 9735-9	-	*Security key and certificate management message (message type - KEYMAN)*
ISO 9735-10		*Security rules for interactive EDI*

Further parts may be added in the future

Introduction

This International Standard includes the rules at the application level for the structuring of data in the interchange of electronic messages in an open environment, based on the requirements of either batch or interactive processing. These rules have been agreed by the United Nations Economic Commission for Europe (UN/ECE) as syntax rules for Electronic Data Interchange for Administration, Commerce and Transport (EDIFACT) and are part of the United Nations Trade Data Interchange Directory (UNTDID) which also includes both batch and interactive Message Design Guidelines.

These syntax rules may be used in any application, but messages using these rules may only be referred to as EDIFACT messages if they comply with other guidelines, rules and directories in the UNTDID. For UN/EDIFACT, messages shall comply with the message design rules for batch or interactive usage as applicable. These rules are maintained in the UNTDID.

Communications specifications and protocols are outside the scope of this standard.

This is a new part, which has been added to ISO 9735. It provides an optional capability of applying confidentiality to an EDIFACT structure i.e. message, package, group or interchange.

ISO 9735-7:1997

Electronic data interchange for administration, commerce and transport (EDIFACT) - Application level syntax rules

Part 7:
Security rules for batch EDI (confidentiality)

1 Scope

This International Standard for batch EDIFACT security addresses message/package level, group level and interchange level security for confidentiality in accordance with established security mechanisms.

2 Conformance

Conformance to a standard means that all of its requirements, including all options, are supported. If all options are not supported, any claim of conformance shall include a statement which identifies those options to which conformance is claimed.

Data that is interchanged is in conformance if the structure and representation of the data conforms to the syntax rules specified in this International Standard.

Devices supporting this International Standard are in conformance when they are capable of creating and/or interpreting the data structured and represented in conformance with the standard.

Conformance shall include conformance to Part 1, Part 2 and Part 5 of this International Standard.

When identified in this International Standard, provisions defined in related standards shall form part of the conformance criteria.

3 Normative references

The following standards contain provisions which, through reference in this text, constitute provisions of this International Standard. All standards are subject to revision, and parties to agreements based on this International Standard are encouraged to investigate the possibility of applying the most recent editions of the standards listed below. Members of IEC and ISO maintain registers of currently valid International Standards.

ISO/IEC 10181-5 Information technology - Security frameworks in Open Systems - Part 5: Confidentiality

4 Definitions

For the purpose of this International Standard, the definitions in Part 1 annex A and in Part 5 annex A apply.

5 Rules for batch EDI confidentiality

5.1 EDIFACT confidentiality

The security threats relevant to EDIFACT data transfer and the security services which address them are described in Part 5 of this International Standard, annexes C and D.

This section describes the solution to provide EDIFACT structures with the security service of confidentiality.

Confidentiality of an EDIFACT structure (message, package, group or interchange) shall be provided by encrypting the message body, object , messages/packages or messages/packages/groups respectively, together with any other security header and trailer segment groups, using an appropriate cryptographic algorithm. This encrypted data may be filtered for use with restricted capability telecommunication networks.

5.1.1 Batch EDI confidentiality

5.1.1.1 Interchange confidentiality

Figure 1 represents the structure of one interchange secured with confidentiality. The service string advice (UNA), the interchange header segment (UNB) and the interchange trailer segment (UNZ) are unaffected by the encryption.

If compression is applied it shall be applied before encryption.

The encryption, compression and filter algorithm and parameters are specified in the security header segment group.

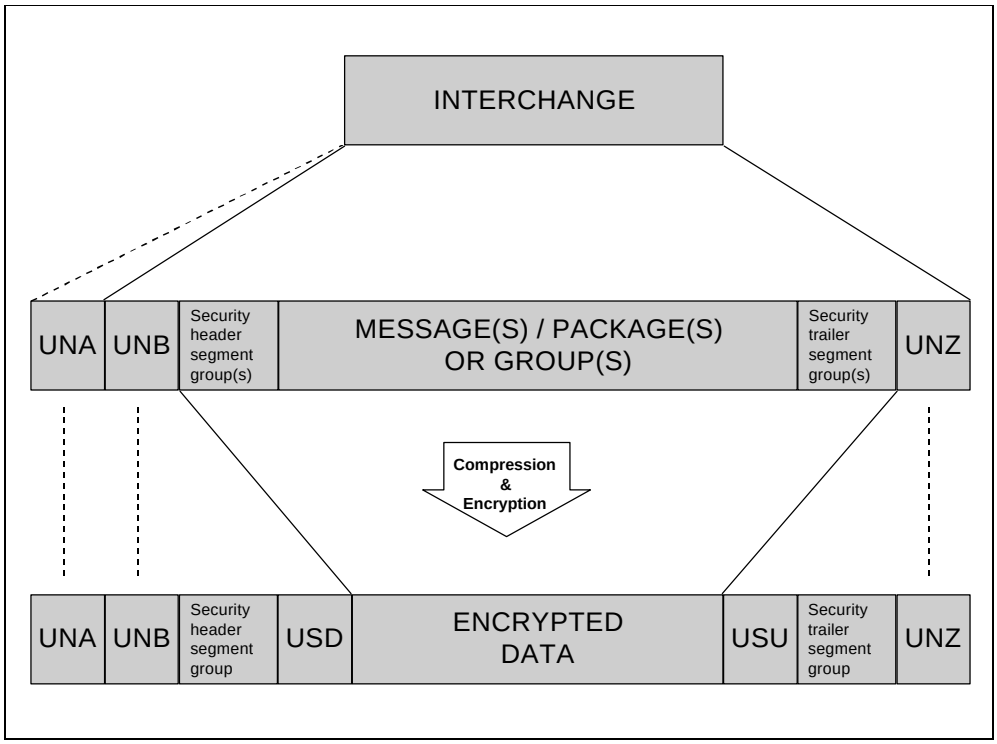

Figure 1 - Structure of an interchange whose contents (message(s)/package(s) or group(s)) have been encrypted (schematic)

5.1.1.2 Group confidentiality

Figure 2 represents the structure of an interchange containing one encrypted group, which has also been secured for other security services. The group header segment (UNG) and the group trailer segment (UNE) are not affected by the encryption.

If compression is applied it shall be applied before encryption.

The encryption, compression and filter algorithm and parameters are specified in the security header segment group.

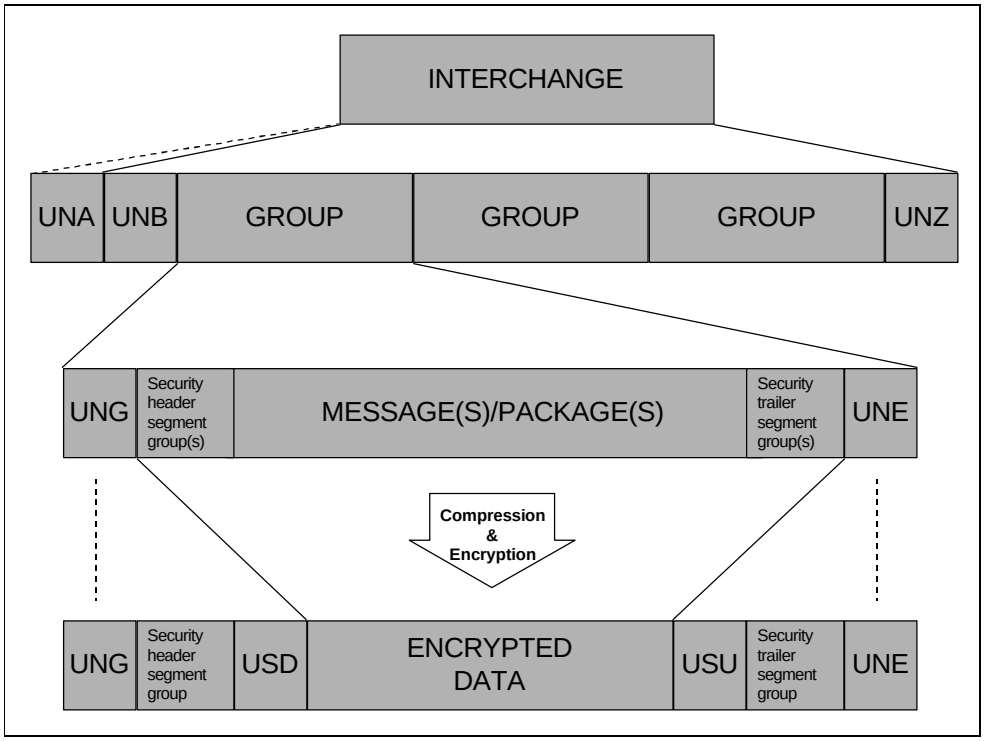

Figure 2 - Structure of an interchange containing one group whose contents (group body and associated security header and trailer segment groups) have been encrypted (schematic)

5.1.1.3 Message confidentiality

Figure 3 represents the structure of an interchange containing one encrypted message, which has also been secured for another security service. The message header segment (UNH) and message trailer segment (UNT) are not affected by the encryption.

If compression is applied it shall be applied before encryption.

The encryption, compression and filter algorithm and parameters are specified in the security header segment group.

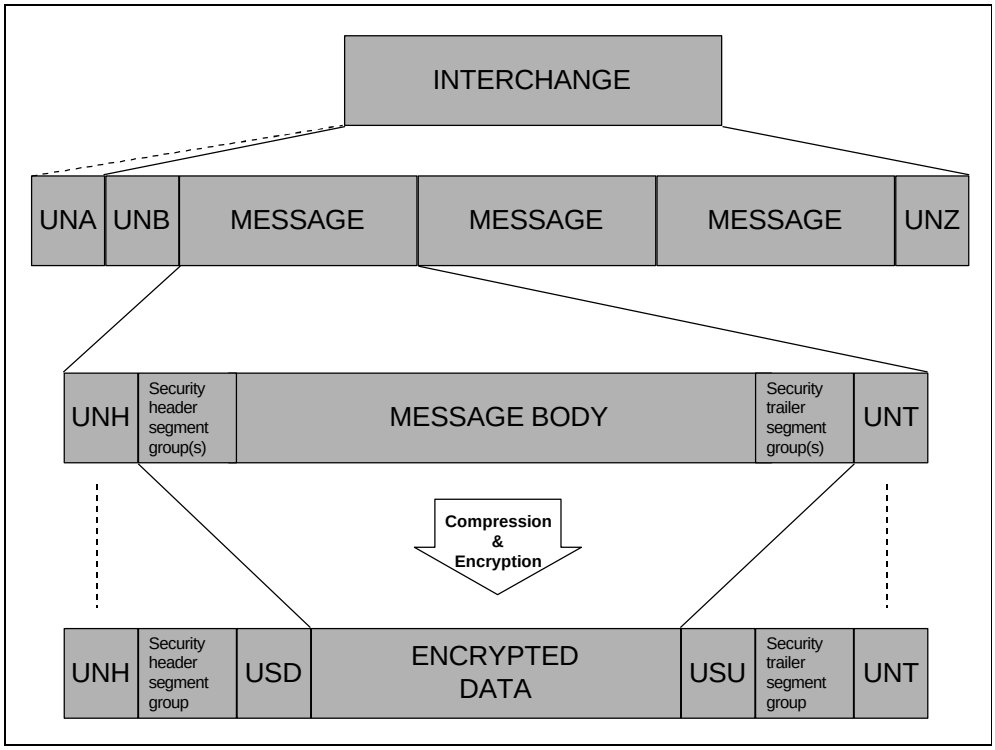

Figure 3 - Structure of an interchange containing one message whose contents (message body and associated security header and trailer segment groups) have been encrypted (schematic)

5.1.1.4 Package confidentiality

Figure 4 represents the structure of an interchange containing one encrypted package, which has also been secured for another security service. The package header segment (UNO) and package trailer segment (UNP) are not affected by the encryption.

If compression is applied it shall be applied before encryption.

The encryption, compression and filter algorithm and parameters are specified in the security header segment group.

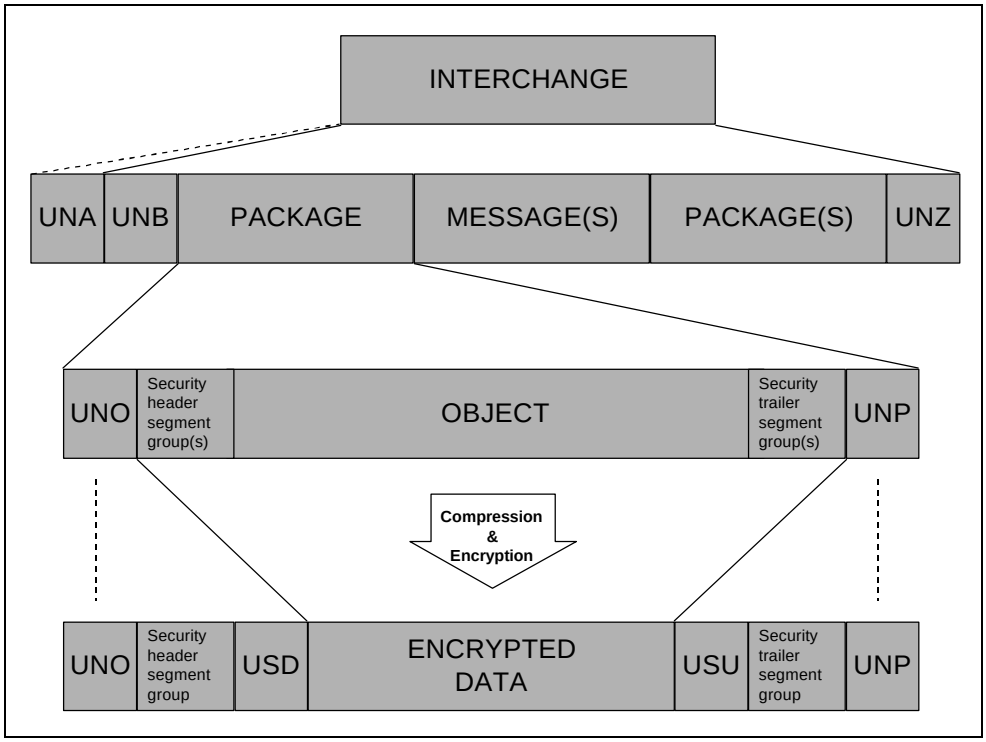

Figure 4 - Structure of an interchange containing one package whose contents (object and associated security header and trailer segment groups) have been encrypted (schematic)

5.1.2 Data encryption header and trailer segment structure

```
TAG     Name                                S   R

-----   Segment Group 1 ----------------    C   99  --------+
USH     Security Header                     M   1           I
USA     Security Algorithm                  C   3           I
-----   Segment Group 2 ----------------    C   2   ----+   I
USC     Certificate                         M   1       I   I
USA     Security Algorithm                  C   3       I   I
USR     Security Result                     C   1   --------+

USD     Data Encryption Header              M   1

        Encrypted data

USU     Data Encryption Trailer             M   1

-----   Segment Group n ----------------    C   99  --------+
UST     Security Trailer                    M   1           I
USR     Security Result                     C   1   --------+
```

Figure 3 - Security header and trailer segment groups segment table

Note: The segments USH, USA, USC, USR and UST are specified in part 5 of this International Standard. They are not described further in this part.

5.1.3 Data segment clarification

Segment Group 1: USH-USA-SG2 (security header segment group)
A group of segments identifying the security service and security mechanisms applied and containing the data necessary to carry out the validation calculations.
There shall be only one security header segment group for confidentiality.

USH, Security header
A segment specifying the security service of confidentiality applied to the EDIFACT structure in which the segment is included (as defined in Part 5).

USA, Security algorithm
A segment identifying a security algorithm, the technical usage made of it, and containing the technical parameters required. This shall be the algorithm(s) applied on the message body, object , messages/packages or messages/packages/groups. These algorithm(s) shall be owner symmetric, owner compressing or owner compression integrity.
Asymmetric algorithms shall not be referred to directly in this USA segment within segment group 1 but may appear only within segment group 2, triggered by a USC segment.

If compression is applied to the data before encryption, an occurrence of USA is used to specify the algorithm and optional mode of operation. Additional parameters, such as initial directory tree, may be specified as parameter value within this USA segment.

If compression is applied and the compression algorithm used does not contain built-in integrity verification, occurrence of an USA segment may be used to specify this. The integrity verification value is calculated over the compressed text before encryption. Location (i.e. octet offset) of the integrity verification value within the compressed data may be specified as a parameter value. The size (in octets of bits) of the integrity verification value is given indirectly by the integrity verification algorithm used.

Segment Group 2: USC-USA-USR (certificate group)
A group of segments containing the data necessary to validate the security methods applied to the

EDIFACT structure, when asymmetric algorithms are used (as defined in Part 5).

USC, Certificate
A segment containing the credentials of the certificate owner and identifying the certification authority which has generated the certificate (as defined in Part 5).

USA, Security algorithm
A segment identifying a security algorithm, the technical usage made of it, and containing the technical parameters required (as defined in Part 5).

USR, Security result
A segment containing the result of the security functions applied to the certificate by the certification authority (as defined in Part 5).

USD, Data encryption header
This segment specifies the size in octets of bits of the compressed (optional), encrypted and filtered (optional) data. A reference number used to identify the encrypted EDIFACT structure may be specified. If a reference number is present the same reference number in both the USD and USU segment shall be used. If padding is applied before encryption, the number of padded octets of bits may be specified.

Encrypted data
This part contains the encrypted data encrypted using the algorithms and mechanisms specified in the security header segment group.

USU, Data encryption trailer
This segment specifies the size in octets of bits of the compressed (optional), encrypted and filtered (optional) data. A reference number used to identify the encrypted EDIFACT structure may be specified. If a reference number is present the same reference number in both the USD and USU segment shall be used.

Segment Group n: UST-USR (security trailer segment group)
A group of segments containing a link with security header segment group and the result of the security functions applied to the EDIFACT structure (as defined in Part 5).

UST, Security trailer
A segment establishing a link between security header and security trailer segment group, and stating the number of security segments contained in these groups, plus the USD and USU segments.

USR, Security result
A segment containing the result of the security functions applied to the EDIFACT structure as specified in the linked security header group (as defined in Part 5). This segment shall not be present for the security service of confidentiality.

5.1.4 Use of data encryption header and data encryption trailer for confidentiality

An EDIFACT structure which is encrypted into encrypted data is packed within a data encryption header and data encryption trailer. The encrypted data and the associated security header and trailer segment groups are replacing the original message body, object or message(s)/package(s)/group(s). The header and trailer of an EDIFACT structure which is encrypted are not affected by the encryption applied.

The encrypted data shall start immediately after the separator ending the USD segment, that shall specify the length of the encrypted data in octets of bits. The encrypted data is followed by a USU segment, that again specifies the length of the encrypted data, which shall be the same as in the USD segment.

5.1.5 Use of security header and security trailer segment groups for confidentiality

As defined in Part 5 of this International Standard, one security header segment group specifying confidentiality and one security trailer segment group shall be included. The security trailer segment group used for confidentiality shall contain only a UST segment.

Once an EDIFACT structure has been encrypted, no other EDIFACT security services shall be provided to it.

5.2 Principles of usage

5.2.1 Multiple security services

If more than one security service is required at the same time, apart from confidentiality, this shall be done, according to the rules defined in Part 5 of this International Standard, before encryption by the party sending the EDIFACT structure, and the related verifications shall be performed after decryption by the receiving party.

5.2.2 Confidentiality

Confidentiality of an EDIFACT structure shall be provided in accordance to the principles defined in ISO 10181-5.

The security service of confidentiality shall be specified in the security header segment group, and the algorithm shall be identified in a USA segment in segment group 1. This USA segment may also contain the data necessary to establish the key relationship between the parties acting as security originator and security recipient.

The party acting as security originator shall encrypt the EDIFACT structure, from immediately after the segment terminator of its header segment (interchange, group, message or package), to immediately before the first character of its segment trailer (interchange, group, message or package), and consider the result as encrypted data. Upon reception of encrypted data, the party acting as security recipient shall decrypt the encrypted data and thus shall recover the original EDIFACT structure, excluding the header and trailer segments.

5.2.3 Internal representation and filter functions

The result of the encryption process is a seemingly random bit-string. This may cause difficulties with certain restricted capability telecommunication networks. To avoid this problem, the bit-string may be reversibly mapped on to a particular character set by means of a filtering function.

The consequence of using a filtering function is to expand the size of the encrypted data. Different filtering functions may be used which have slightly different expansion factors. Some may allow the filtered text to contain any character of the target character set, including service characters such as segment terminators, whereas other filter functions may filter out these service characters.

The length of data conveyed in the data element “length of data in octets of bits” in the USD and USU segments shall represent the length of the (compressed,) encrypted (and filtered) data. This shall be used to determine the end of the encrypted data. The filter function used shall be indicated in 0505 (filter function, coded) of the USH in the confidentiality security header segment group.

5.2.4 Use of compression techniques before encryption

The computing cost of encryption being directly related to the size of the data to encrypt, it may be useful to compress the data before encryption.

Most compression techniques would not be efficient on encrypted text, even filtered, thus if compression is required, it shall be applied before encryption.

Consequently, when it is used for the confidentiality security service, the security header segment group may contain the indication that data have been compressed before encryption, and may identify the compression algorithm and optional parameters used. In such a case, after decryption of the encrypted data, the data shall be decompressed before the EDIFACT structure is recovered.

5.2.5 Processing order of operations

5.2.5.1 Encryption and related operations

When processing an EDIFACT structure to provide confidentiality, operations shall be performed as follows:

1. compress the EDIFACT structure (optional) and calculate integrity value on the compressed data (optional)
2. encrypt the (compressed and integrity protected) EDIFACT structure
3. filter the (compressed and integrity protected) encrypted data (optional)

5.2.5.2 Decryption and related operations

When processing an encrypted EDIFACT structure to recover an original EDIFACT structure, operations shall be performed as follows:

1. unfilter the filtered encrypted data (if filtered)
2. decrypt the encrypted data
3. verify integrity value on the compressed data (if integrity value is present) and expand (i.e. decompress) the decrypted data to recover the original EDIFACT structure (if compressed)

Annex A
(normative)
Addendum - to be added to Part 1 annex C when approved

Syntax service directories
(segments, composite data elements and simple data elements)

A.1. Segment directory

A.1.1 Segment directory specification legend:

Function — The function of the segment

POS — The sequential position number of the stand-alone data element or composite data element in the segment table

TAG — The tags of all service segments contained in the segment directory start with the letter “U”. The tags of all service composite data elements start with the letter "S", and the tags of all service simple data elements start with the figure "0"

Name — Name of a COMPOSITE DATA ELEMENT in capital letters
Name of a STAND-ALONE DATA ELEMENT in capital letters
Name of a component data element in small letters

S — The status of the stand-alone data element or composite data element in the segment, or of the components in the composite (where M = Mandatory and C = Conditional)

R — The maximum number of occurrences of a stand-alone data element or composite data element in the segment

Repr. — Data value representation of the stand-alone data element or component data elements in the composite.

a	alphabetic characters
n	numeric characters
an	alphanumeric characters
a3	3 alphabetic characters, fixed length
n3	3 numeric characters, fixed length
an3	3 alphanumeric characters, fixed length
a..3	up to 3 alphabetic characters
n..3	up to 3 numeric characters
an..3	up to 3 alphanumeric characters

A.1.2 Dependency note identifiers

Code	Name
D1	One and only one
D2	All or none
D3	One or more
D4	One or none
D5	If first, then all
D6	If first, then at least one more
D7	If first, then none of the others

See clause 11.5 in Part 1 for the definition of the dependency note identifiers.

A.1.3 Index of segments by tag

TAG	Name
USD	Data encryption header
USU	Data encryption trailer

A.1.4 Index of segments by name

TAG	Name
USD	Data encryption header
USU	Data encryption trailer

A.1.5 Segment specifications

Note:

Only segments not defined in other parts of this International standard are included here.

USD DATA ENCRYPTION HEADER

Function: To specify size (i.e. length of data in octets of bits) of encrypted data following the segment terminator of this segment.

POS	TAG	Name	S	R	Repr.	Notes
010	0556	LENGTH OF DATA IN OCTETS OF BITS	M	1	n..18	
020	0518	ENCRYPTION REFERENCE NUMBER	C	1	an..35	
030	0582	NUMBER OF PADDING BYTES	C	1	n..2	

USU DATA ENCRYPTION TRAILER

Function: To provide a trailer for the encrypted data.

POS	TAG	Name	S	R	Repr.	Notes
010	0556	LENGTH OF DATA IN OCTETS OF BITS	M	1	n..18	1
020	0518	ENCRYPTION REFERENCE NUMBER	C	1	an..35	2

NOTES:

1. 0556, the value shall be identical to the value in 0556 in the corresponding USD segment.

2. 0518, the value shall be identical to the value in 0518 in the corresponding USD segment.

A.3 Simple data element directory

A.3.1 Simple data element specification legend:

The tags of all service simple data elements contained in the simple data element directory start with the figure “0”.

Name Name of a simple data element

Desc. Description of the simple data element

Repr. Data value representation of the simple data element:

a	alphabetic characters
n	numeric characters
an	alphanumeric characters
a3	3 alphabetic characters, fixed length
n3	3 numeric characters, fixed length
an3	3 alphanumeric characters, fixed length
a..3	up to 3 alphabetic characters
n..3	up to 3 numeric characters
an..3	up to 3 alphanumeric characters

A.3.2 Index of simple data elements by tag

TAG	Name
0518	Encryption reference number
0556	Length of data in octets of bits
0582	Number of padding bytes

A.3.3 Index of simple data elements by name

TAG	Name
0518	Encryption reference number
0556	Length of data in octets of bits
0582	Number of padding bytes

A.3.4 Simple data element specifications

Note:

Only simple data elements not defined in other parts of this International standard are included here.

```
---------------------------------------------------------------------------

   0518  ENCRYPTION REFERENCE NUMBER

   Desc: Reference number to the encrypted EDIFACT structure.

   Repr: an..35

---------------------------------------------------------------------------

   0556  LENGTH OF DATA IN OCTETS OF BITS

   Desc: A count of the data octets of bits.

   Repr: n..18

---------------------------------------------------------------------------

   0582  NUMBER OF PADDING BYTES

   Desc: Count of the number of padding bytes.

   Repr: n..2

---------------------------------------------------------------------------
```

Annex B
(informative)

Message protection example

One example is provided herein to illustrate application of security service segments.

This example of message confidentiality is based on fictive EDIFACT payment orders. The security mechanisms described here are totally independent of the type of message and may be applied to any EDIFACT message.

This example shows how security service segments may be used when a**symmetric algorithm** based method is applied, to provide message content confidentiality. The symmetric key has been exchanged previously between the partners, and the security header segment group contains only two rather simple segments.

B.1 Narrative

Company A orders Bank A, sort code 603000 to debit its account number 00387806 on April 9th 1995 in the amount of 54345.10 Pounds Sterling. The amount is to be paid to Bank B, sort code 201827, in favour of account number 00663151 of Company B, West Dock, Milford Haven. The payment is in settlement of invoice 62345. The contact name at the Beneficiary is Mr. Jones in the Sales Department.

Bank A requires the payment order to be secured by the security service "message confidentiality".
This is achieved by encrypting the message body with the symmetric "Data Encryption Standard" (DES) at the message sender's side. It is assumed that the secret DES-key has previously been exchanged between Company A and Bank A. To reduce size of transmitted information the message body is compressed before encryption is applied. The algorithm used to compress the message body is ISO 12042.

B.1 Security details

In the following, only the confidentiality security header and trailer segment groups will be referred to.

SECURITY HEADER	
SECURITY SERVICE	Message confidentiality
SECURITY REFERENCE NUMBER	The reference of this header is 1
FILTER FUNCTION	All binary values are filtered with hexadecimal filter
ORIGINAL CHARACTER SET ENCODING	The message was coded in ASCII 8 bits when as encrypted.
SECURITY IDENTIFICATION DETAILS Message sender (party which encrypts the message).	Mr. SMITH of Company A
SECURITY IDENTIFICATION DETAILS Message receiver (party which decrypts the message).	Bank A
SECURITY SEQUENCE NUMBER	The security sequence number of this message is 001
SECURITY DATE AND TIME	The security time stamp is: date: 1995 04 09 time: 13:59:50
SECURITY ALGORITHM	

ISO 9735-7:1997

SECURITY ALGORITHM Use of algorithm Cryptographic mode of operation algorithm Padding algorithm	 A symmetric algorithm is used to achieve Message confidentiality A Cipher Block Chaining mode is used. DES algorithm is used. Binary 0 is used as padding scheme.
ALGORITHM PARAMETER Algorithm parameter qualifier Algorithm parameter value	 Identifies this algorithm parameter value as the name of a previously exchanged symmetric key. The key called ENC-KEY1 is used.
SECURITY ALGORITHM	
SECURITY ALGORITHM Use of algorithm Algorithm	 A compression algorithm is used to reduce message size before encryption An ISO 12042 compression algorithm is used.
ENCRYPTION HEADER	
Length of data in octets of bits Encryption reference number Number of padding bytes	The size of the compressed, encrypted and filtered message body. The reference number is 1. The number of padding bytes are 4.
Encrypted data	
Encrypted data	Compressed, encrypted and filtered message body.
ENCRYPTION TRAILER	
Length of data in octets of bits Encryption reference number	The size of the compressed, encrypted and filtered message body. The reference number is 1.
SECURITY TRAILER	
NUMBER OF SECURITY SEGMENTS	The value 6. (USH, USA, USA, USD, USU, UST)
SECURITY REFERENCE NUMBER	The reference of this security trailer is 1

Annex C
(informative)

Processing example

C.1 Encryption example

The diagram in figure 5 is a processing example. Implementations may choose to have different sequence and realisations of the different components.

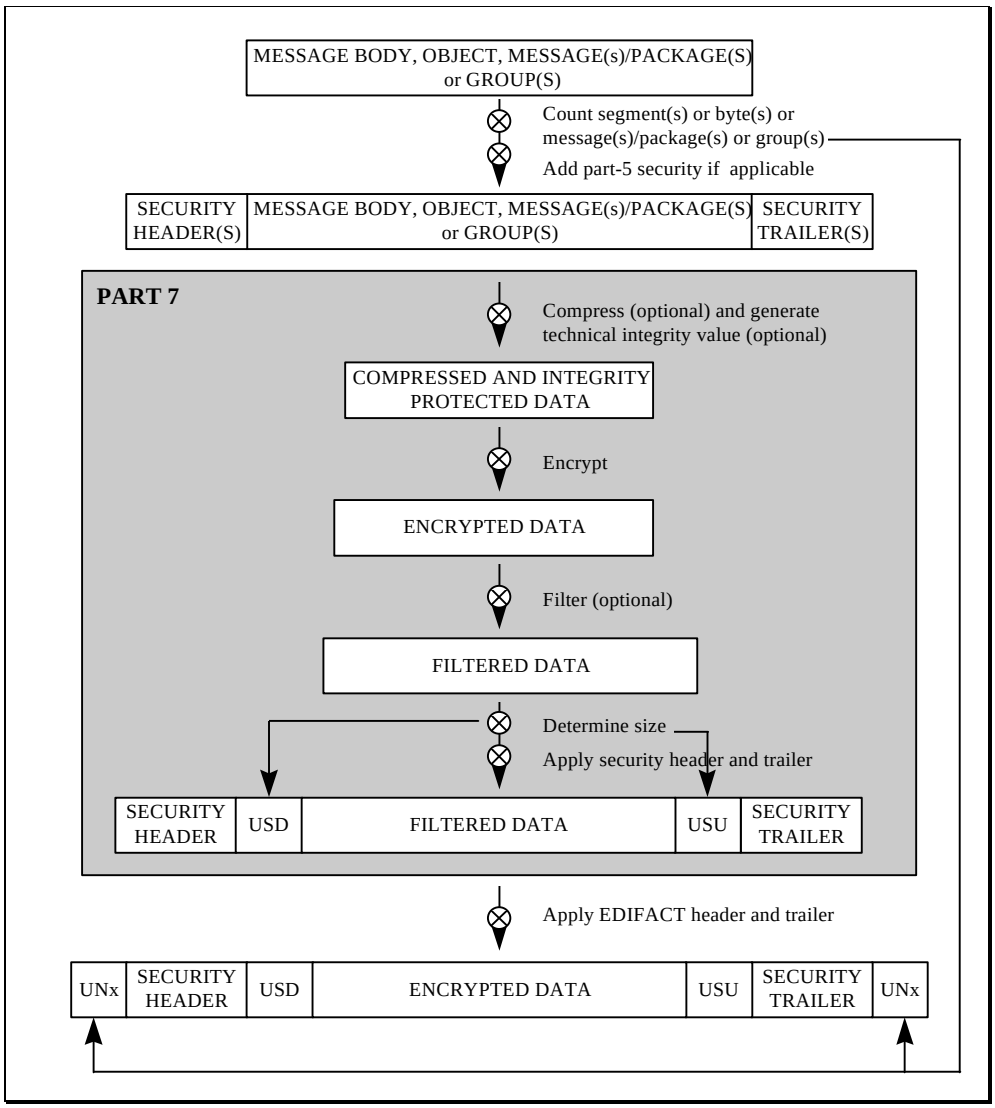

Figure 5 - Processes involved in encryption of an EDIFACT structure.

C.2 Decryption example

The diagram in figure 5 is a processing example. Implementations may choose to have different sequence and realisations of the different components.

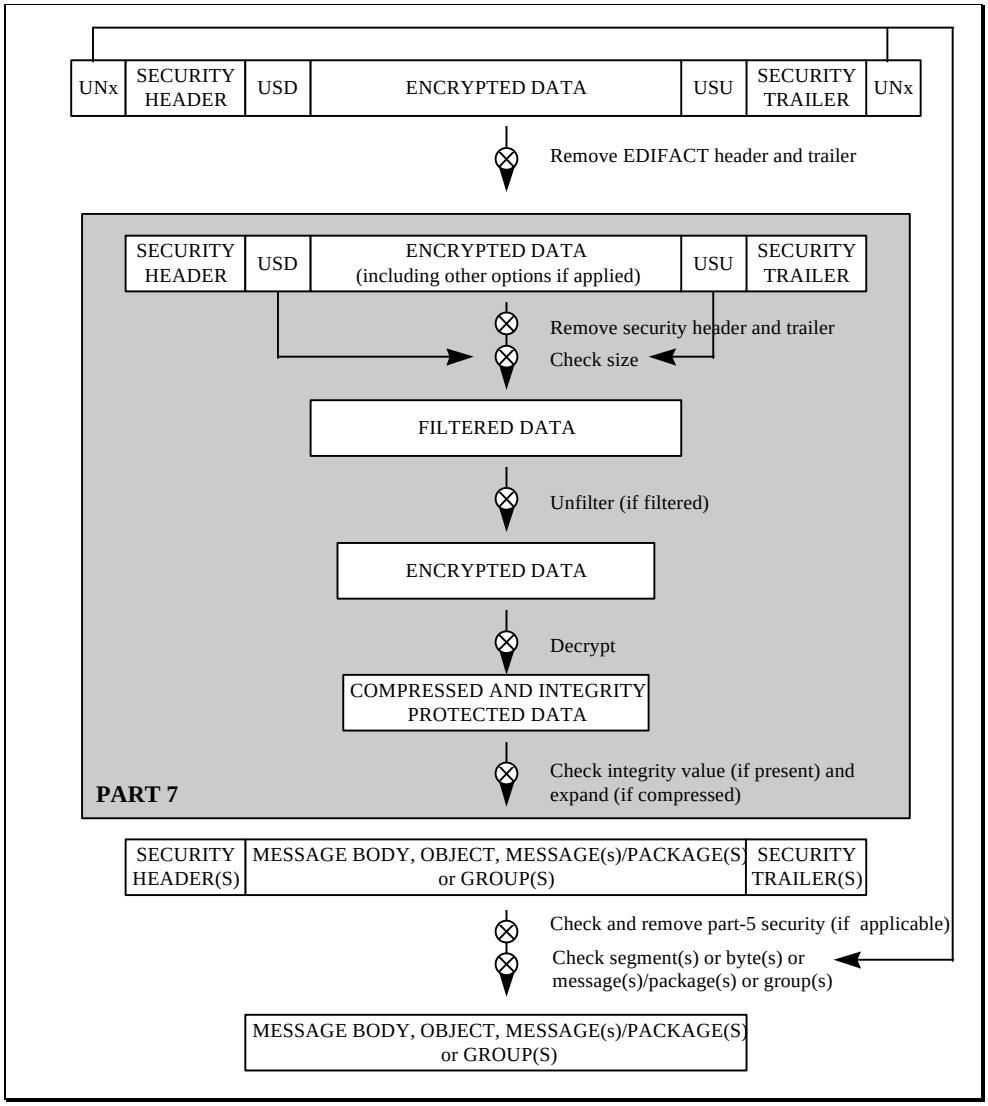

Figure 6 - Processes involved in decryption of an EDIFACT structure.

Annex D
(informative)
Confidentiality service and algorithms

D.1 Purpose and scope

Annex D gives examples of possible combinations of data elements and code values from the security segment groups. These examples have been chosen to illustrate some widely used security techniques, based on international standards.

The full set of possible combinations is far too large to be presented in this annex. The choices made here must not be considered as an endorsement of the algorithms or modes of operation. The user is invited to choose the techniques appropriate to the security threats he wants to be protected against.

The purpose of this annex is to provide the user, once he has chosen the security techniques, with a comprehensive starting point to work out a suitable solution for his particular application.

List of codes used in the matrixes (subset of the complete code list)

0501	***Security service, coded***
4	Confidentiality

0523	***Use of algorithm, coded***
3	Issuer signing
4	Issuer hashing
5	Owner enciphering
8	Owner compressing
9	Owner compression integrity

0525	***Cryptographic mode of operation, coded***
2	CBC (DES mode or operation)
16	DSMR (Digital signature scheme giving message recovery)
18	CBC-TBSS (DES mode of operation with TBSS padding)
19	RSA-TBSS (Enveloping using RSA with TBSS padding)
36	CTS (RC5 mode of operation)

0527	***Algorithm, coded***
1	DES (Data Encryption Standard)
4	IDEA (International Data Encryption Algorithm)
10	RSA
14	RIPEMD-160 (Dedicated Hash-Function #1)
18	ZLIB (Data compression algorithm)
25	CRC-32 (Cyclic redundancy check)
27	ISO12042 (data compression)
29	RC5 (Variable-Key Size Symmetric Block Cipher)

0531	***Algorithm parameter qualifier***
5	Symmetric key, encrypted under a symmetric key
6	Symmetric key, encrypted under a public key
9	Symmetric key name
10	Key encrypting key name
12	Modulus
13	Exponent
14	Modulus length

0563	***Validation value qualifier***
1	Unique validation value

0577	***Security party qualifier***
1	Message sender
2	Message receiver
3	Certificate owner
4	Authenticating party

0589	***Padding algorithm, coded***
1	Zero padding
2	PKCS #1 padding
4	TBSS padding

Abbreviations, used

a123, 1, ABC99	=	Representations of a Security Reference Number
CA	=	Certification Authority
CA-Sig	=	CA-Signature
Enc-Key	=	Encrypted Key
Exp	=	Public exponent
KEK-N	=	Key encrypting key name
Key-N	=	Key Name
Len	=	Length in octets of bits of (compressed,) encrypted (and filtered) data
Mod	=	Public modulus
Mod-L	=	Length of Public modulus
PK/CA	=	Public Key of Certification Authority

D.2 Combinations using symmetric algorithms and integrated security segments to reach confidentiality of an EDIFACT structure

The following matrix establishes the relationships for the specific cases of

- integrated message/package/group/interchange level security (ISO 9735 part 7)
- use of symmetric algorithms for encryption
- use of symmetric and asymmetric algorithms for key exchange
- security services provided are confidentiality
- confidentiality is provided using DES, IDEA and RC5 algorithms. Three examples are given,
    1. DES in CBC mode with a secret key known by the recipient. The secret key needed is encrypted under a key-encrypting-key shared between sender and receiver. This key-encrypting-key is referred to by its name. There is no data compression applied. The padding scheme used is zero-padding and requires additional information on the number of padding bytes.
    2. RC5 in CTS mode with a secret key known by the recipient. The secret key needed is encrypted under a key-encrypting-key shared between sender and receiver. This key-encrypting-key is referred to by its name. ISO 12042 compression is applied before encryption is applied.
    3. IDEA in CBC mode with TBSS padding applied. The secret key used for encryption is exchanged using the public key of the recipient. The public key is embedded in a certificate. Z-lib compression and CRC-32 integrity protection is applied before encryption.
- although sender and receiver share keys, the cryptographic mechanisms have not been completely agreed beforehand. Therefore all the algorithms and mode of operation used are explicitly named.
- only the security fields related to security techniques, algorithms and modes of operation actually used are shown.
- the USC segment contains explicitly the identification of the hash function and the signature function used by the Certification Authority to sign the certificate. The public key of Certification Authority, needed to check the certificate signature is already known by the receiver. It is referred to by name in the USC segment.

TAG	**Name**	**S**	**R**	Confidentiality Example 1	Confidentiality Example 2	Confidentiality Example 3	Notes
SG 1		C	99	one per security service			1
USH	SECURITY HEADER	M	1				
0501	SECURITY SERVICE, CODED	M		4	4	4	

TAG	Name	S	R	Confidentiality Example 1	Confidentiality Example 2	Confidentiality Example 3	Notes
0534	SECURITY REFERENCE NUMBER	M		a123	1	ABC99	
S500	SECURITY IDENTIFICATION DETAILS	C	2	(Sender)			
0577	Security party qualifier	M		1	1	1	
0511	Security party identification	C		Id of sender	Id of sender	Id of sender	
S500	SECURITY IDENTIFICATION DETAILS	C	2	(Recipient)			
0577	Security party qualifier	M		2	2	2	
0511	Security party identification	C		Id of recipient	Id of recipient	Id of recipient	
USA	SECURITY ALGORITHM	C	3	(Encryption algorithm)			
S502	SECURITY ALGORITHM	M	1				
0523	Use of algorithm, coded	M		5	5	5	
0525	Cryptographic mode of operation, coded	C		2	36	18	
0527	Algorithm, coded	C		1	29	4	
0589	Padding algorithm, coded	C		1	2	4	2
S503	ALGORITHM PARAMETER	C	9	One for encrypted key			
0531	Algorithm parameter qualifier	M		5	5	6	
0554	Algorithm parameter value	M		Key	Key	Key	
S503	ALGORITHM PARAMETER	C	9	One for key-encrypting-key name			
0531	Algorithm parameter qualifier	M		10	10	-	
0554	Algorithm parameter value	M		Key-N	Key-N	-	
USA	SECURITY ALGORITHM	C	3	(Compression algorithm)			
S502	SECURITY ALGORITHM	M	1				
0523	Use of algorithm, coded	M		-	8	8	
0525	Cryptographic mode of operation, coded	C		-	-	-	
0527	Algorithm, coded	C		-	27	18	
USA	SECURITY ALGORITHM	C	3	(Compression integrity algorithm)			
S502	SECURITY ALGORITHM	M	1				
0523	Use of algorithm, coded	M		-	-	9	
0525	Cryptographic mode of operation, coded	C		-	-	-	
0527	Algorithm, coded	C		-	-	25	
SG 2		C	2	only one: recipient certificate			
USC	CERTIFICATE	M	1				
S500	SECURITY IDENTIFICATION DETAILS	C	2	(certificate owner)			
0577	Security party qualifier	M		-	-	3	
0511	Security party identification	C		-	-	Id of owner	
S500	SECURITY IDENTIFICATION DETAILS	C	2	(authenticating party)			
0577	Security party qualifier	M		-	-	4	
0538	Key name	C		-	-	(PK/CA name)	
0511	Security party identification	C		-	-	Id of CA	
USA	SECURITY ALGORITHM	C	3	(CA’s hash function for certificate's signature)			
S502	SECURITY ALGORITHM	M	1				
0523	Use of algorithm, coded	M		-	-	4	
0525	Cryptographic mode of operation, coded	C		-	-	-	

TAG	Name	S	R	Confidentiality Example 1	Confidentiality Example 2	Confidentiality Example 3	Notes
0527	Algorithm, coded	C		-	-	14	
USA	SECURITY ALGORITHM	C	3	(CA's signature function for certificate's signature)			
S502	SECURITY ALGORITHM	M	1				
0523	Use of algorithm, coded	M		-	-	3	
0525	Cryptographic mode of operation, coded	C		-	-	16	
0527	Algorithm, coded	C		-	-	10	
S503	Algorithm parameter	C	9	(CA public key modulus)			
0531	Algorithm parameter qualifier	M		-	-	12	
0554	Algorithm parameter value	M		-	-	Mod	
S503	Algorithm parameter	C	9	(CA public key exponent)			
0531	Algorithm parameter qualifier	M		-	-	13	
0554	Algorithm parameter value	M		-	-	Exp	
S503	Algorithm parameter	C	9	(CA public key modulus length)			
0531	Algorithm parameter qualifier	M		-	-	14	
0554	Algorithm parameter value	M		-	-	Mod-L	
USA	SECURITY ALGORITHM	C	3	(Certificate owner's encryption function)			
S502	SECURITY ALGORITHM	M	1				
0523	Use of algorithm, coded	M		-	-	5	
0525	Cryptographic mode of operation, coded	C		-	-	19	
0527	Algorithm, coded	C		-	-	10	
S503	Algorithm parameter	C	9	(Owner public key modulus)			
0531	Algorithm parameter qualifier	M		-	-	12	
0554	Algorithm parameter value	M		-	-	Mod	
S503	Algorithm parameter	C	9	(Owner public key exponent)			
0531	Algorithm parameter qualifier	M		-	-	13	
0554	Algorithm parameter value	M		-	-	Exp	
S503	Algorithm parameter	C	9	(Owner public key modulus length)			
0531	Algorithm parameter qualifier	M		-	-	14	
0554	Algorithm parameter value	M		-	-	Mod-L	
USR	SECURITY RESULT	C	1				
S508	VALIDATION RESULT	M	2				
0563	Validation value qualifier	M		-	-	1	
0560	Validation value	C		-	-	CA-Sig	
USD	DATA ENCRYPTION HEADER	M	1				
0556	Length of data in octets of bits	M	1	Len	Len	Len	
0518	Encryption reference number	C	1	-	A	-	
0582	Number of padding bytes	C	1	3	-	-	3
Data structures to be secured (message body, object, message(s)/package(s)/group(s))							
USU	DATA ENCRYPTION TRAILER	M	1				
0556	Length of data in octets of bits	M	1				
0518	Encryption reference number	C	1	-	A	-	
SG n		C	99	one per security service			1
UST	SECURITY TRAILER	M	1				
0534	SECURITY REFERENCE NUMBER	M		a123	1	ABC99	

TAG	Name	S	R	Confidentiality Example 1	Confidentiality Example 2	Confidentiality Example 3	Notes
0588	Number of security segments	M	1	5	6	12	

Figure 1 - Matrix of relationship

Notes:
1. both structures must have the same occurrence number
2. padding only applies to USA segment specifying the encryption algorithm
3. the number of padding bytes is chosen as an example