Joint ISO/TC 154 – UN/CEFACT Syntax Working Group (JSWG) publication of ISO 9735-7

equivalent to the official ISO publication: ISO 9735-7 **(Second edition 2002-07-01)**

Electronic data interchange for administration, commerce and transport (EDIFACT) — Application level syntax rules (Syntax version number: 4, Syntax release number: 1) —

Part 7:

Security rules for batch EDI (confidentiality)

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide 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 organizations, 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 standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 3.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this part of ISO 9735 may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO 9735-7 was prepared by Technical Committee ISO/TC 154, *Processes, data elements and documents in commerce, industry and administration* in collaboration with UN/CEFACT through the Joint Syntax Working Group (JSWG).

This second edition cancels and replaces the first edition (ISO 9735-7:1999). However ISO 9735:1988 and its Amendment 1:1992 are provisionally retained for the reasons given in clause 2.

Furthermore, for maintenance reasons the Syntax service directories have been removed from this and all other parts of the ISO 9735 series. They are now consolidated in a new part, ISO 9735-10.

At the time of publication of ISO 9735-1:1998, ISO 9735-10 had been allocated as a part for “Security rules for interactive EDI”. This was subsequently withdrawn because of lack of user support, and as a result, all relevant references to the title “Security rules for interactive EDI” were removed in this second edition of ISO 9735-7.

Definitions from all parts of the ISO 9735 series have been consolidated and included in ISO 9735-1.

ISO 9735 consists of the following parts, under the general title *Electronic data interchange for administration, commerce and transport (EDIFACT) — Application level syntax rules (Syntax version number: 4, Syntax release number: 1)*:

— *Part 1: Syntax rules common to all parts*

— *Part 2: Syntax rules specific to batch EDI*

— *Part 3: Syntax rules specific to interactive EDI*

— *Part 4: Syntax and service report message for batch EDI (message type — CONTRL)*

— *Part 5: Security rules for batch EDI (authenticity, integrity and non-repudiation of origin)*

— *Part 6: Secure authentication and acknowledgement message (message type — AUTACK)*

— *Part 7: Security rules for batch EDI (confidentiality)*

— *Part 8: Associated data in EDI*

— *Part 9: Security key and certificate management message (message type — KEYMAN)*

— *Part 10: Syntax service directories*

Further parts may be added in the future.

Annexes A to C of this part of ISO 9735 are for information only.

Introduction

This part of ISO 9735 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.

This part of ISO 9735 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 part of ISO 9735.

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.

Electronic data interchange for administration, commerce and transport (EDIFACT) — Application level syntax rules (Syntax version number: 4, Syntax release number: 1) —

Part 7:
Security rules for batch EDI (confidentiality)

1 Scope

This part of ISO 9735 for batch EDIFACT security addresses message/package level, group level and interchange level security for confidentiality in accordance with established security mechanisms.

2 Conformance

Whereas this part shall use a version number of “4” in the mandatory data element 0002 (Syntax version number), and shall use a release number of “01” in the conditional data element 0076 (Syntax release number), each of which appear in the segment UNB (Interchange header), interchanges continuing to use the syntax defined in the earlier published versions shall use the following Syntax version numbers, in order to differentiate them from each other and from this part:

— ISO 9735:1988 — *Syntax version number: 1*

— ISO 9735:1988 (amended and reprinted in 1990) — *Syntax version number: 2*

— ISO 9735:1988 and its Amendment 1:1992 — *Syntax version number: 3*

— ISO 9735:1998 — *Syntax version number: 4*

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 part of ISO 9735.

Devices supporting this part of ISO 9735 are in conformance when they are capable of creating and/or interpreting the data structured and represented in conformance with the standard.

Conformance to this part shall include conformance to parts 1, 2, 5 and 10 of ISO 9735.

When identified in this part of ISO 9735, provisions defined in related standards shall form part of the conformance criteria.

3 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this part of ISO 9735. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this part of ISO 9735 are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies. Members of ISO and IEC maintain registers of currently valid International Standards.

ISO 9735-1:2002, *Electronic data interchange for administration, commerce and transport (EDIFACT) — Application level syntax rules (Syntax version number: 4, Syntax release number: 1) — Part 1: Syntax rules common to all parts*

ISO 9735-2:2002, *Electronic data interchange for administration, commerce and transport (EDIFACT) — Application level syntax rules (Syntax version number: 4, Syntax release number: 1) — Part 2: Syntax rules specific to batch EDI*

ISO 9735-5:2002, *Electronic data interchange for administration, commerce and transport (EDIFACT) — Application level syntax rules (Syntax version number: 4, Syntax release number: 1) — Part 5: Security rules for batch EDI (authenticity, integrity and non-repudiation of origin)*

ISO 9735-10:2002, *Electronic data interchange for administration, commerce and transport (EDIFACT) — Application level syntax rules (Syntax version number: 4, Syntax release number: 1) — Part 10: Syntax service directories*

ISO/IEC 10181-5:1996, *Information technology — Open Systems Interconnection — Security frameworks for open systems: Confidentiality framework*

4 Terms and definitions

For the purposes of this part of ISO 9735, the terms and definitions given in ISO 9735-1 apply.

5 Rules for batch EDI confidentiality

5.1 EDIFACT confidentiality

5.1.1 General

The security threats relevant to EDIFACT data transfer and the security services which address them are described in ISO 9735-5:2002, annexes A and B.

This clause 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.

5.1.2 Batch EDI confidentiality

5.1.2.1 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.

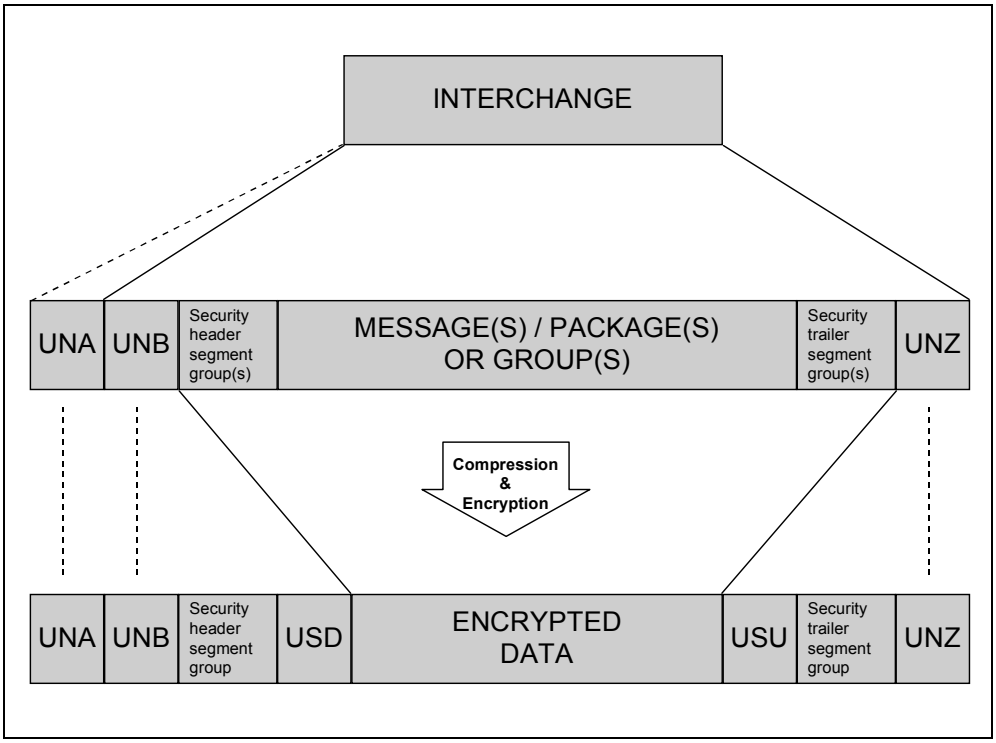

Figure 1 — Structure of an interchange whose contents [message(s)/package(s) or group(s)] have been encrypted (schematic)

5.1.2.2 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.

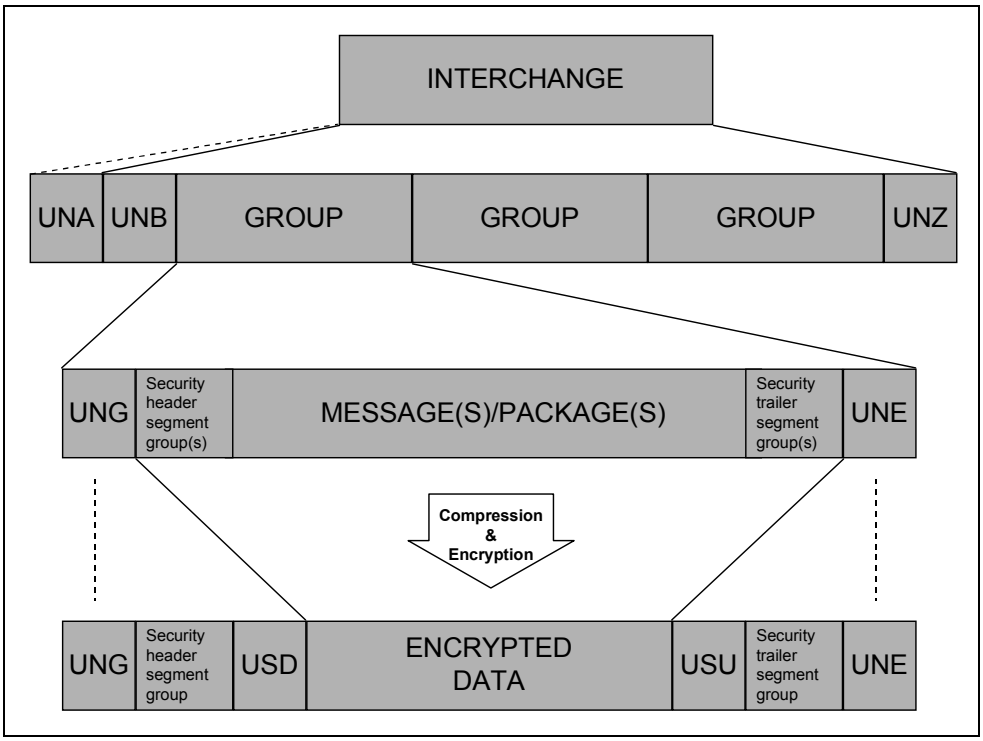

Figure 2 — Structure of an interchange containing one group whose contents (group body and associated security header and trailer segment groups) have been encrypted (schematic)

5.1.2.3 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.

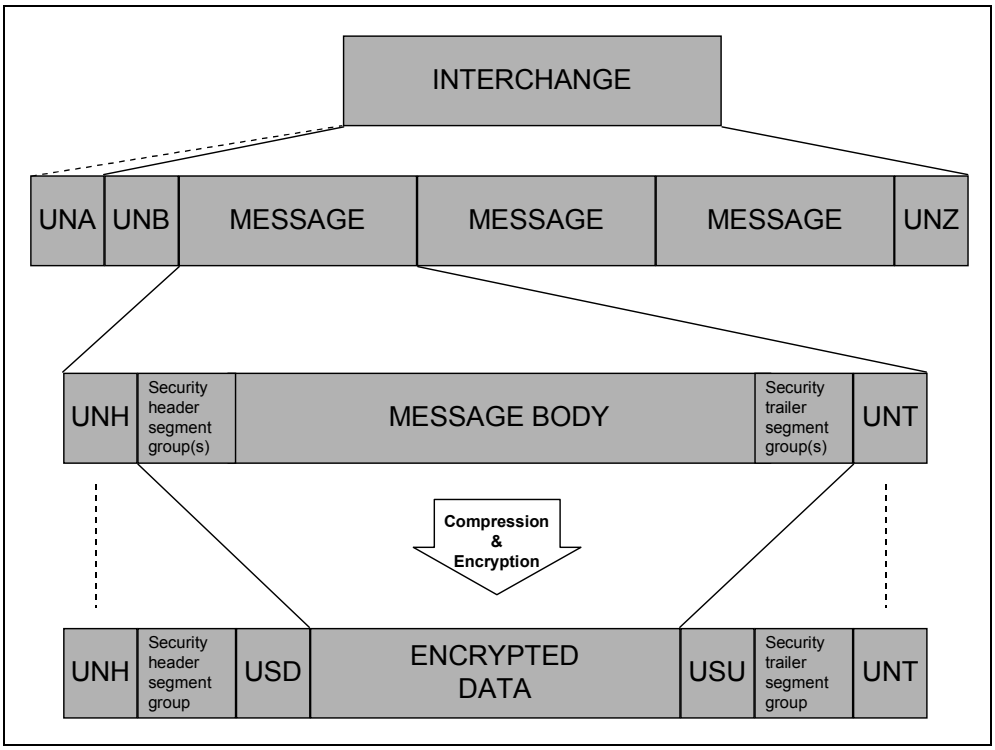

Figure 3 — Structure of an interchange containing one message whose contents (message body and associated security header and trailer segment groups) have been encrypted (schematic)

5.1.2.4 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.

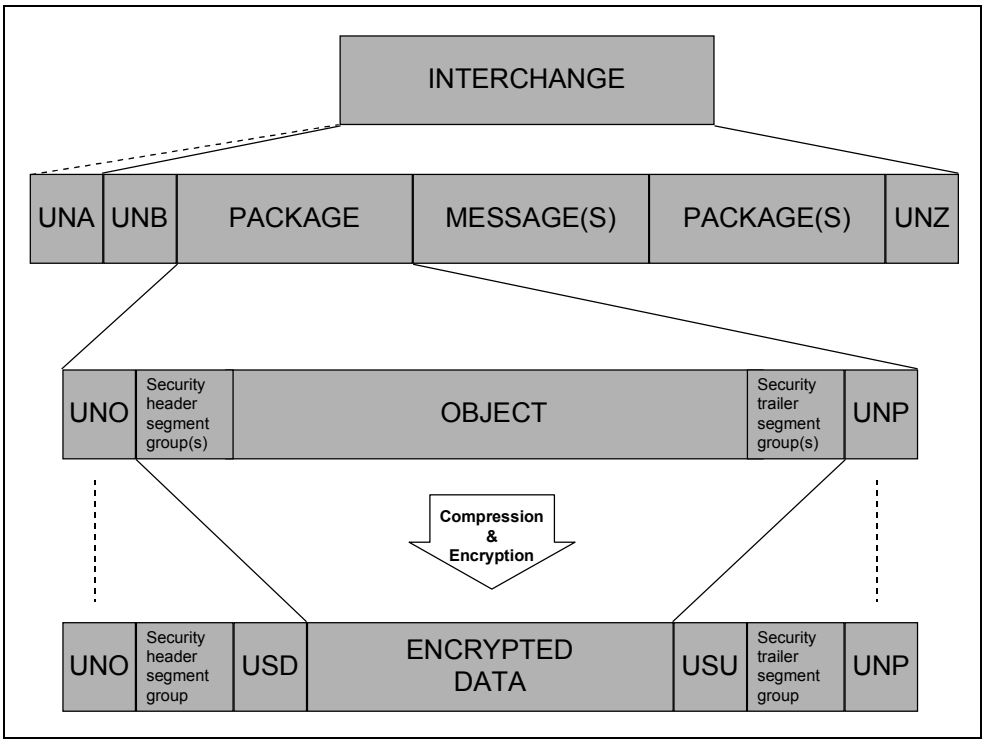

Figure 4 — Structure of an interchange containing one package whose contents (object and associated security header and trailer segment groups) have been encrypted (schematic)

5.1.3 Data encryption header and trailer segment structure

Table 1 — Security header and trailer segment groups segment table

TAG	Name	S	R	
———	Segment Group 1 ———————	C	99	——————┐
USH	Security Header	M	1	│
USA	Security Algorithm	C	3	│
———	Segment Group 2 ———————	C	2	———┐ │
USC	Certificate	M	1	│ │
USA	Security Algorithm	C	3	│ │
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	│
USR	Security Result	C	1	——————┘

NOTE The segments USH, USA, USC, USR and UST are specified in ISO 9735-10. They are not described further in this part of ISO 9735.

5.1.4 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 ISO 9735-5).

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 ISO 9735-5).

USC, Certificate

A segment containing the credentials of the certificate owner and identifying the certification authority which has generated the certificate (as defined in ISO 9735-5).

USA, Security algorithm

A segment identifying a security algorithm, the technical usage made of it, and containing the technical parameters required (as defined in ISO 9735-5).

USR, Security result

A segment containing the result of the security functions applied to the certificate by the certification authority (as defined in ISO 9735-5).

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 ISO 9735-5).

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 ISO 9735-5). This segment shall not be present for the security service of confidentiality.

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

An EDIFACT structure, which is transformed 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 that 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.

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

As defined in ISO 9735-5, 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 ISO 9735-5, before encryption by the party sending the EDIFACT structure. The receiving party shall perform the related verifications after decryption.

5.2.2 Confidentiality

Confidentiality of an EDIFACT structure shall be provided in accordance to the principles defined in ISO/IEC 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
(informative)

Message protection example

A.1 Introduction

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.

A.2 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/IEC 12042:1993, *Information technology — Data compression for information interchange — Binary arithmetic coding algorithm.*

A.3 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	
SECURITY ALGORITHM	
Use of algorithm	A symmetric algorithm is used to achieve Message confidentiality.
Cryptographic mode of operation	A Cipher Block Chaining mode is used.
Algorithm	DES algorithm is used.
Padding mechanism	Binary 0 is used as padding scheme.
ALGORITHM PARAMETER	
Algorithm parameter qualifier	Identifies this algorithm parameter value as the name of a previously exchanged symmetric key.
Algorithm parameter value	The key called ENC-KEY1 is used.
SECURITY ALGORITHM	
SECURITY ALGORITHM	
Use of algorithm	A compression algorithm is used to reduce message size before encryption.
Algorithm	An ISO 12042 compression algorithm is used.
ENCRYPTION HEADER	
LENGTH OF DATA IN OCTETS OF BITS	The size of the compressed, encrypted and filtered message body.
ENCRYPTION REFERENCE NUMBER	The reference number is 1.
NUMBER OF PADDING BYTES	The number of padding bytes is 4.
Encrypted data	
Encrypted data	Compressed, encrypted and filtered message body
ENCRYPTION TRAILER	
LENGTH OF DATA IN OCTETS OF BITS	The size of the compressed, encrypted and filtered message body.
ENCRYPTION REFERENCE NUMBER	The reference number is 1.
SECURITY TRAILER	
NUMBER OF SECURITY SEGMENTS	The value is 6. (USH, USA, USA, USD, USU, UST)
SECURITY REFERENCE NUMBER	The reference of this security trailer is 1.

Annex B
(informative)

Processing example

B.1 Encryption example

The diagram in Figure B.1 is a processing example. Implementations may choose to have different sequence and realizations of the different components.

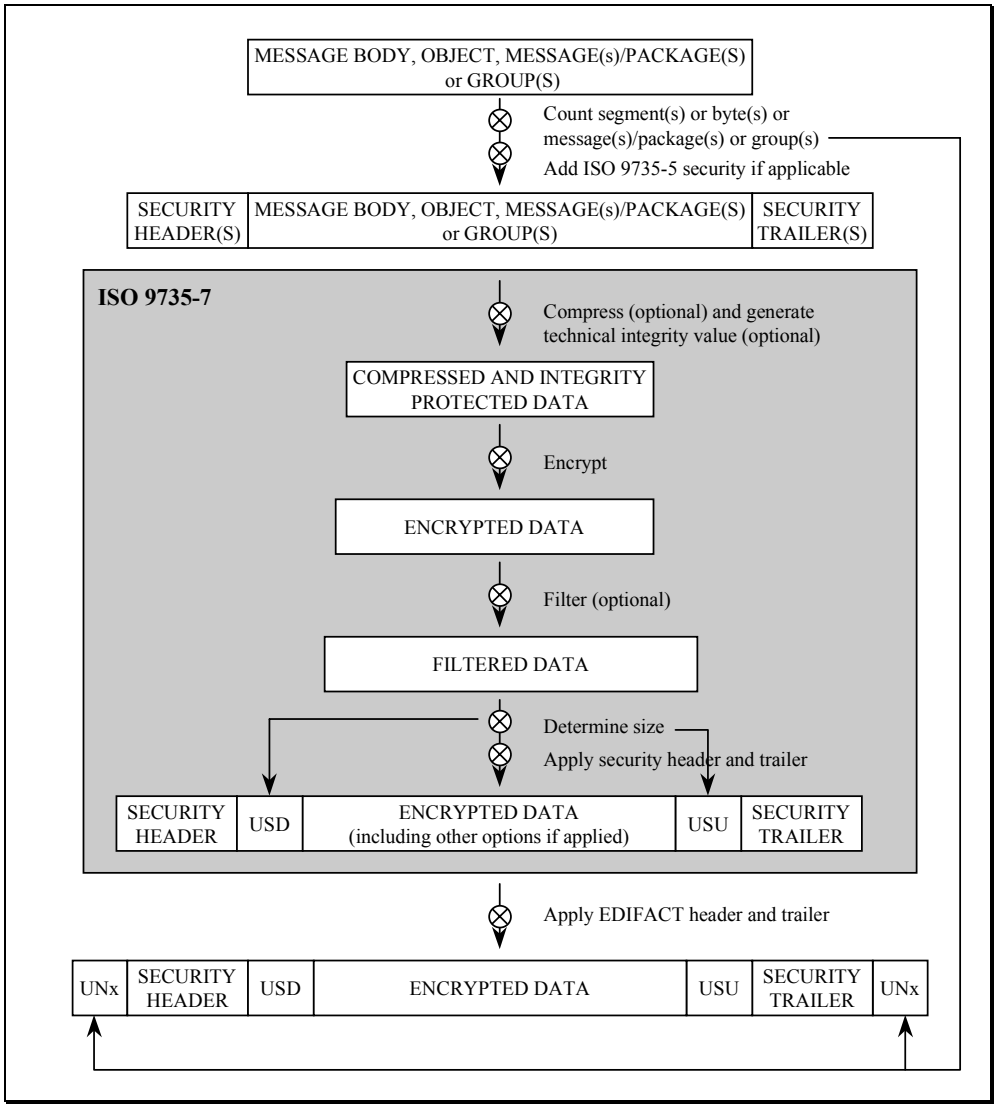

Figure B.1 — Processes involved in encryption of an EDIFACT structure

B.2 Decryption example

The diagram in Figure B.2 is a processing example. Implementations may choose to have different sequence and realizations of the different components.

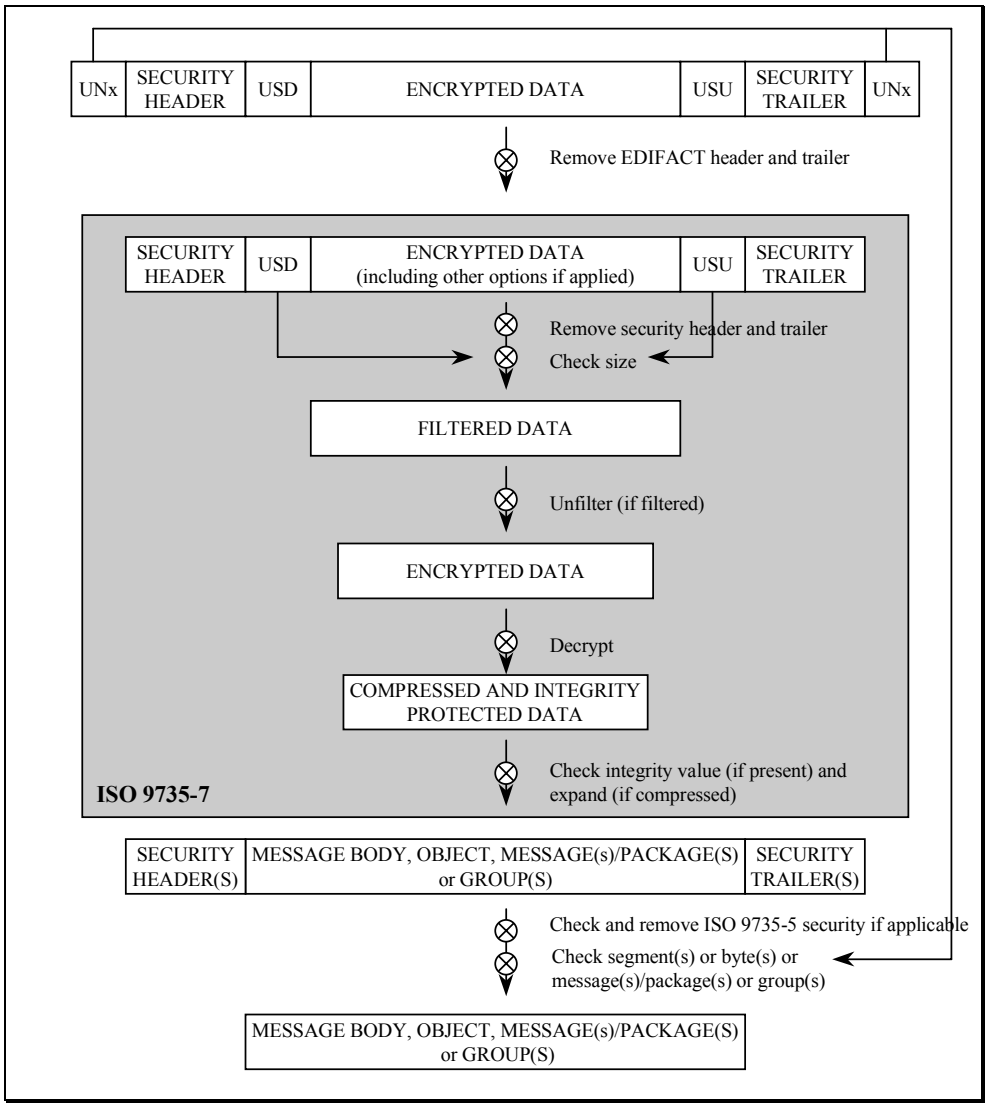

Figure B.2 — Processes involved in decryption of an EDIFACT structure

Annex C
(informative)

Confidentiality service and algorithms

C.1 Purpose and scope

This annex 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 of operation)
16	DSMR (Digital signature scheme giving message recovery)
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

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

12	Modulus
13	Exponent
14	Modulus length

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

0591	***Padding mechanism, 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
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

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

The matrix given in Table C.1 establishes the relationships for the specific cases of

— integrated message/package/group/interchange level security (ISO 9735-7),

— 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. 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.

Table C.1 — Matrix of relationships

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	1	4	4	4	
0534	SECURITY REFERENCE NUMBER	M	1	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	2	
0527	Algorithm, coded	C		1	29	4	
0591	Padding mechanism, 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	

TAG	Name	S	R	Confidentiality Example 1	Confidentiality Example 2	Confidentiality Example 3	Notes
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		—	—	—	
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		—	—	—	
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	

TAG	Name	S	R	Confidentiality Example 1	Confidentiality Example 2	Confidentiality Example 3	Notes
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	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	
0588	NUMBER OF SECURITY SEGMENTS	M	1	5	6	12	

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.