

Australian Standard™

**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**



Standards Australia



Documents

Document Sharing Hub

This Australian Standard was prepared by Committee IT-001, Information systems—Interconnection. It was approved on behalf of the Council of Standards Australia on 30 March 2003 and published on 14 May 2003.

The following are represented on Committee IT-001:

Australian Bureau of Statistics
Australian Communications Industry Forum
Australian Information Industry Association
Australian Telecommunications Users Group
Australian Vice-Chancellors' Committee
Electrical Compliance Testing Association
Information Technology Association of New Zealand

Keeping Standards up-to-date

Standards are living documents which reflect progress in science, technology and systems. To maintain their currency, all Standards are periodically reviewed, and new editions are published. Between editions, amendments may be issued. Standards may also be withdrawn. It is important that readers assure themselves they are using a current Standard, which should include any amendments which may have been published since the Standard was purchased.

Detailed information about Standards can be found by visiting the Standards Australia web site at www.standards.com.au and looking up the relevant Standard in the on-line catalogue.

Alternatively, the printed Catalogue provides information current at 1 January each year, and the monthly magazine, *The Australian Standard*, has a full listing of revisions and amendments published each month.

We also welcome suggestions for improvement in our Standards, and especially encourage readers to notify us immediately of any apparent inaccuracies or ambiguities. Contact us via email at mail@standards.com.au, or write to the Chief Executive, Standards Australia International Ltd, GPO Box 5420, Sydney, NSW 2001.

This Standard was issued in draft form for comment as DR 03043.

Australian Standard™

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

First published as AS ISO 9735.5—2003.

COPYRIGHT

© Standards Australia International

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher.

Published by Standards Australia International Ltd
GPO Box 5420, Sydney, NSW 2001, Australia

ISBN 0 7337 5204 7

PREFACE

This Standard was prepared by the Australian members of the Joint Standards Australia/Standards New Zealand Committee IT-001, Information systems—Interconnection. After consultation with stakeholders in both countries, Standards Australia and Standards New Zealand decided to develop this Standard as an Australian, rather than an Australian/New Zealand Standard.

This Standard is identical with, and has been reproduced from, 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*.

The objective of this Standard is to specify syntax rules for EDIFACT security and to provide a method to address message/package level, group level and interchange level security for authenticity, integrity and non-repudiation of origin, in accordance with established security mechanisms.

This Standard is Part 5 of AS ISO 9735—2003, *Electronic data interchange for administration, commerce and transport (EDIFACT)—Application level syntax rules (Syntax version number: 4, Syntax release number: 1)*, which is published in parts as follows:

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 (this Standard)

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

The terms ‘normative’ and ‘informative’ are used to define the application of the annex to which they apply. A normative annex is an integral part of a standard, whereas an informative annex is only for information and guidance.

As this Standard is reproduced from an international standard, the following applies:

- (a) Its number appears on the cover and title page while the international standard number appears only on the cover.
- (b) In the source text ‘this International Standard’ should read ‘this Australian Standard’.
- (c) A full point substitutes for a comma when referring to a decimal marker.

References to International Standards should be replaced by references to Australian or Australian/New Zealand Standards, as follows:

Reference to International Standard

ISO

9735 Electronic data interchange for administration, commerce and transport (EDIFACT)—Application level syntax rules (Syntax version number: 4, Syntax release number: 1)

9735-1 Part 1: Syntax rules common to all parts

Australian Standard

AS ISO

9735 Electronic data interchange for administration, commerce and transport (EDIFACT)—Application level syntax rules (Syntax version number: 4, Syntax release number: 1)

9735.1 Part 1: Syntax rules common to all parts

ISO		AS ISO	
9735-2	Part 2: Syntax rules specific to batch EDI	9735.2	Part 2: Syntax rules specific to batch EDI
9735-6	Part 6: Secure authentication and acknowledgement message (message type—AUTACK)	9735.6	Part 6: Secure authentication and acknowledgement message—message type—AUTACK
9735-7	Part 7: Security rules for batch EDI (confidentiality)	9735.7	Part 7: Security rules for batch EDI—confidentiality
9735-8	Part 8: Associated data in EDI	9735.8	Part 8: Associated data in EDI
9735-10	Part 10: Syntax service directories	9735-10	Part 10: Syntax service directories

CONTENTS

Page

1	Scope	1
2	Conformance.....	1
3	Normative references	2
4	Terms and definitions	2
5	Rules for the use of security header and trailer segment groups for batch EDI	2
6	Rules for the use of interchange and group security header and trailer segment groups for batch EDI	10
	Annex A (informative) EDIFACT security threats and solutions	14
	Annex B (informative) How to protect an EDIFACT structure	17
	Annex C (informative) Message protection examples.....	20
	Annex D (informative) Filter functions for UN/EDIFACT character set repertoires A and C	28
	Annex E (informative) Security services and algorithms.....	31
	Bibliography	38

AUSTRALIAN STANDARD

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)

1 Scope

This part of ISO 9735 specifies syntax rules for EDIFACT security. It provides a method to address message/package level, group level and interchange level security for authenticity, integrity and non-repudiation of origin, 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 conform 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 this part of ISO 9735.

Conformance to this part of ISO 9735 shall include conformance to parts 1, 2, 8 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 9735-6:2002, *Electronic data interchange for administration, commerce and transport (EDIFACT) — Application level syntax rules (Syntax version number: 4, Syntax release number: 1) — Part 6: Secure authentication and acknowledgement message (message type — AUTACK)*

ISO 9735-7:2002, *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)*

ISO 9735-8:2002, *Electronic data interchange for administration, commerce and transport (EDIFACT) — Application level syntax rules (Syntax version number: 4, Syntax release number: 1) — Part 8: Associated data in EDI*

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 10181-2:1996, *Information technology — Open Systems Interconnection — Security frameworks for open systems: Authentication framework*

ISO/IEC 10181-4:1997, *Information technology — Open Systems Interconnection — Security frameworks for open systems: Non-repudiation framework*

ISO/IEC 10181-6:1996, *Information technology — Open Systems Interconnection — Security frameworks for open systems: Integrity 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 the use of security header and trailer segment groups for batch EDI

5.1 Message/package level security — integrated message/package security

5.1.1 General

The security threats relevant to message/package transmission and the security services which address them are described in annexes A and B.

This subclause describes the structure of EDIFACT message/package level security.

Security services addressed in this part of ISO 9735 shall be provided by the inclusion of security header and trailer segment groups after the UNH and before the UNT, in a way which shall be applied to any existing message, or after the UNO and before the UNP, for any existing package.

5.1.2 Security header and trailer segment groups

Figure 1 describes an interchange showing security at message level.

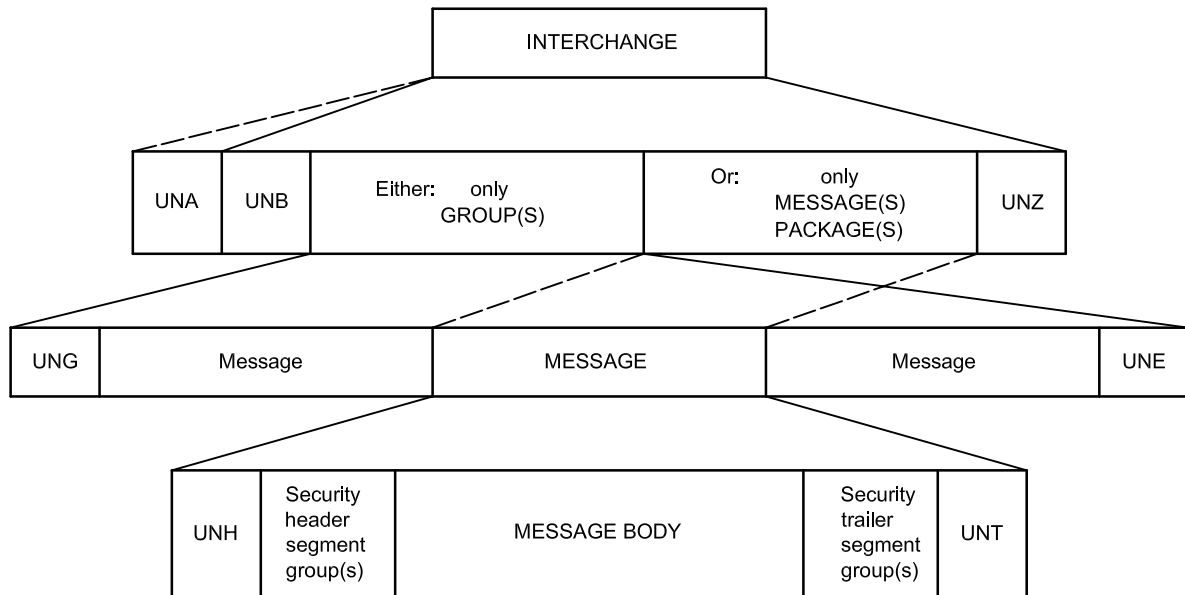


Figure 1 — Interchange showing security at message level (schematic)

Figure 2 describes an interchange showing security at package level.

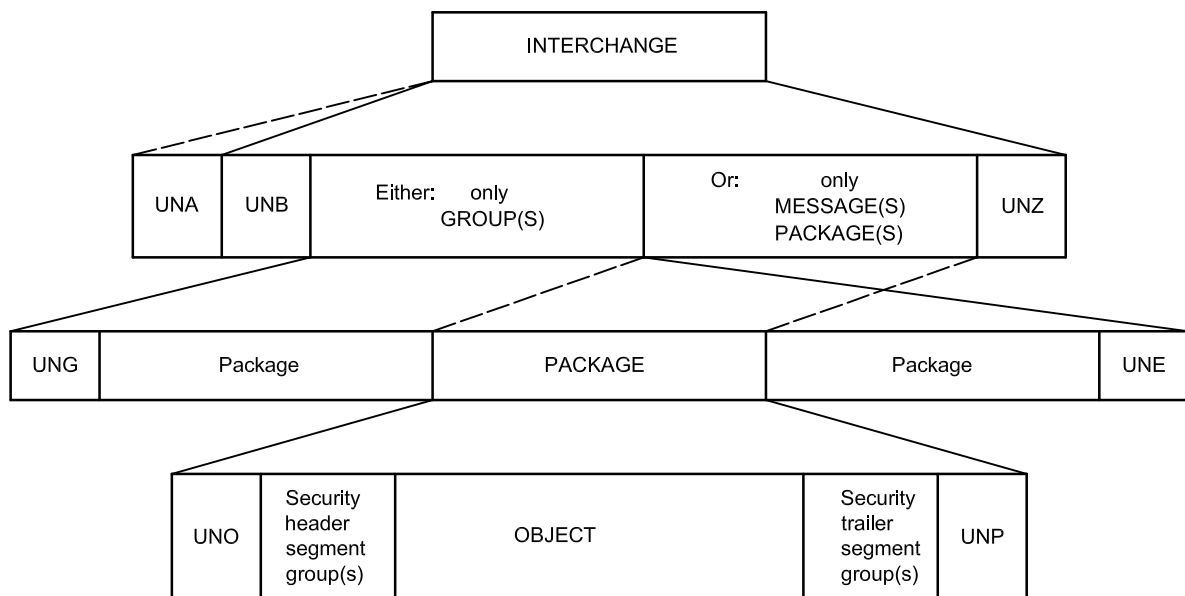


Figure 2 — Interchange showing security at package level (schematic)

5.1.3 Security header and trailer segment groups structure

Table 1 — Security header and security trailer segment groups segment table (message level security)

TAG	Name	S	R
UNH	Message Header	M	1
-----	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 -----+
	Message body		
-----	Segment Group n -----	C	99 ----+
UST	Security Trailer	M	1 I
USR	Security Result	C	1 ----+
UNT	Message Trailer	M	1

Table 2 — Security header and security trailer segment groups segment table (package level security)

TAG	Name	S	R
UNO	Object Header	M	1
-----	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 -----+
	Object		
-----	Segment Group n -----	C	99 ----+
UST	Security Trailer	M	1 I
USR	Security Result	C	1 ----+
UNP	Object Trailer	M	1

NOTE The complete directory specification of the segments and data elements, including segments UNH message header, UNT message trailer, UNO object header and UNP object trailer 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 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 may be several different security header segment groups within the same message/package, if different security services are applied to the message/package (e. g. integrity and non-repudiation of origin) or if the same security service is applied by several parties.

USH, Security header

A segment specifying a security service applied to the message/package in which the segment is included.

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 either:

- if symmetric algorithms are used, or
- if 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 parties.

This 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.

USH segment may specify the filter function used for the binary fields of USA segment within segment group 1 and of the USR segment of the corresponding security trailer group.

USH segment may include a security sequence number, to provide sequence integrity, and the date of creation of the security elements.

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 applied directly on the message/package. This algorithm may be either symmetric, a hash function or a compression algorithm. For example, for a digital signature, it indicates the message-dependent hash function to be used.

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.

Three occurrences of the USA segment are allowed. One occurrence shall be used for the symmetric algorithm or the hash function required to provide the security service specified in the USH segment. The other two occurrences are described in ISO 9735-7.

Indication of padding mechanism may be used when appropriate.

Segment Group 2: USC-USA-USR (certificate group)

A group of segments containing the data necessary to validate the security methods applied to the message/package, when asymmetric algorithms are used. Certificate segment group shall be used when asymmetric algorithms are used to identify the asymmetric key pair used, even if certificates are not used.

Either the full certificate segment group (including the USR segment), or the only data elements necessary to identify unambiguously the asymmetric key pair used, shall be present in the USC segment. The presence of a full

certificate may be avoided if the certificate has already been exchanged by the two parties, or if it may be retrieved from a database.

Where it is decided to refer to a non-EDIFACT certificate (such as X.509), the certificate syntax and version shall be identified in data element 0545 of the USC segment. Such certificates may be conveyed in an EDIFACT package.

Two occurrences of this segment group are allowed, one being the message/package sender certificate (that the message/package receiver will use to verify the sender's signature), the other being the message/package receiver certificate (only referred to by certificate reference) in the case where the receiver public key is used by the sender for confidentiality of symmetric keys.

If both are present within one security header segment group, the security identification details composite data element (S500) together with the certificate reference data element (0536) allow them to be differentiated.

This segment group shall be omitted if no asymmetric algorithm is used.

USC, Certificate

A segment containing the credentials of the certificate owner and identifying the certification authority which has generated the certificate. The data element filter function, coded (0505) shall identify the filter function used for the binary fields of USA segments and USR segment within segment group 2.

USC certificate may contain two occurrences of S500: one for the certificate owner (identifying the party which signs with the private key associated to the public key contained in this certificate), one for the certificate issuer (certification authority or CA).

USA, Security algorithm

A segment identifying a security algorithm, the technical usage made of it, and containing the technical parameters required. The three different occurrences of this USA segment in segment group 2 are identifying:

- 1 the algorithm used by the certificate issuer to compute the hash value of the certificate (hashing function);
- 2 the algorithm used by the certificate issuer to generate the certificate (i.e. to sign the result of the hash function computed on the certificate content) (asymmetric algorithm);
- 3a - either the algorithm used by the sender to sign the message/package (i.e. to sign the result of the hash function described in the USH segment, computed on the message/package content) (asymmetric algorithm);
- 3b - or the receiver's asymmetric algorithm used by the sender to encrypt the key required by a symmetric algorithm applied to the message/package content and referred to by the segment group 1 triggered by the USH segment (asymmetric algorithm).

Indication of padding mechanism may be used when appropriate.

USR, Security result

A segment containing the result of the security functions applied to the certificate by the certification authority. This result shall be the signature of the certificate computed by the certification authority by signing the hash result computed on the data of the credentials.

For the certificate, the signature computation starts with the first character of the USC segment (namely the "U") and ends with the last character of the last USA segment (including the separator following this USA segment).

Segment Group n: UST-USR (security trailer group)

A group of segments containing a link with security header segment group and the result of the security functions applied to the message/package.

UST, Security trailer

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

USR, Security result

A segment containing the result of the security functions applied to the message/package as specified in the linked security header group. Depending on the security mechanisms specified in the linked security header group, this result shall be either:

- computed directly on the message/package by the algorithm specified in the USA segment within segment group 1 of the security header group, or
- computed by signing with an asymmetric algorithm specified in USA segment within segment group 2 of the security header segment group a hash result computed on the message/package by the algorithm specified in the USA segment within segment group 1 of the security header segment group.

5.1.5 Scope of security application

There are two possibilities for the scope of security application:

1. The computation of each of the integrity and authentication values and of the digital signatures starts with and includes the current security header segment group and the message body, or object, itself. In this case no other security header or security trailer segment groups shall be encompassed within this scope.

The security header segment group shall be counted from the first character, namely a “U”, to the separator ending this security header segment group, both included, and the message body, or object, from the first character following the separator ending the last security header segment group to the separator preceding the first character of the first security trailer segment group, both included.

Thus the order in which security services integrated in this manner are performed, is not prescribed. They are completely independent of each other.

Figure 3 illustrates this case (the scope of application of the security service defined in the security header 2 is represented by shaded boxes).

UNH/ UNO	Security header segment group 3	Security header segment group 2	Security header segment group 1	MESSAGE BODY/ OBJECT	Security trailer segment group 1	Security trailer segment group 2	Security trailer segment group 3	UNT/ UNP
-------------	--	--	--	-------------------------	---	---	---	-------------

Figure 3 — Scope of application: security header segment group and message body/object only (schematic)

2. The computation starts with and includes the current security header segment group to the associated security trailer segment group. In this case the current security header segment group, the message body, or object, and all the other embedded security header and trailer segment groups shall be encompassed within this scope.

The scope shall include every character from the first character, namely a “U”, of the current security header segment group, to the separator preceding the first character of the associated security trailer segment group, both included.

Figure 4 illustrates this case (the scope of application of the security service defined in the security header 2 is represented by shaded boxes).

UNH/ UNO	Security header segment group 3	Security header segment group 2	Security header segment group 1	MESSAGE BODY/ OBJECT	Security trailer segment group 1	Security trailer segment group 2	Security trailer segment group 3	UNT/ UNP
-------------	--	--	--	-------------------------	---	---	---	-------------

Figure 4 — Scope of application: from security header segment group to security trailer segment group (schematic)

For each added security service, either of the two approaches may be chosen.

In both cases, the relation between the security header segment group and associated security trailer segment group shall be provided by the data elements security reference number of the USH and of the UST segments.

5.2 Principles of usage

5.2.1 Choice of service

The security header segment group may include the following general information:

- security service applied;
- identification of the parties involved;
- security mechanism used;
- “unique” value (sequence number and/or timestamp);
- non-repudiation of receipt request.

If more than one security service is required for the same EDIFACT structure, then the security header segment group may be present several times. This shall be the case when several pairs of parties are involved. However, if several services are required between the same two parties they may be included in a single pair of security header and trailer segment groups, as certain services include others implicitly.

5.2.2 Authenticity

If origin authentication of a EDIFACT structure is required, it shall be provided in accordance to the principles defined in ISO/IEC 10181-2, using an appropriate pair of security header and security trailer segment groups.

The security service of origin authentication shall be specified in the USH segment and the algorithm shall be identified in the USA segment in segment group 1. It shall be a symmetric algorithm.

The party acting as security originator shall compute an authenticity value that shall be conveyed in the USR segment of the security trailer segment group. The party acting as security recipient shall check the authenticity value.

This service may include integrity service and may be obtained as a subproduct of non-repudiation of origin service.

If an appropriate implementation of this “origin authentication” service, based on tamper resistant hardware or trusted third parties, is used, it may be considered as an instance of “non repudiation of origin” service. Such a practice shall be defined in the interchange agreement.

5.2.3 Integrity

If content integrity of a EDIFACT structure is required, it shall be provided in accordance to the principles defined in ISO/IEC 10181-6, using an appropriate pair of security header and security trailer segment groups.

The security service of integrity shall be specified in the USH segment and the algorithm shall be identified in the USA segment in segment group 1. It shall be hash function or a symmetric algorithm.

The party acting as security originator shall compute an integrity value that shall be conveyed in the USR segment of the security trailer segment group. The party acting as security recipient shall check the integrity value.

This service may be obtained as a subproduct of origin authentication service or of non-repudiation of origin service.

If sequence integrity is required, either a security sequence number or a security timestamp, or both, shall be contained by the security header segment group and either content integrity service or origin authentication service or non-repudiation of origin service shall be used.

5.2.4 Non-repudiation of origin

If non-repudiation of origin of a EDIFACT structure is required, it shall be provided in accordance to the principles defined in ISO/IEC 10181-4, using an appropriate pair of security header and security trailer segment groups.

The security service of non-repudiation of origin shall be specified in the USH segment and the hashing algorithm shall be identified in the USA segment in segment group 1, and the asymmetric algorithm used for signature in the USA segments of segment group 2, if certificates are used.

If the certificate is not conveyed in the message/package, the asymmetric algorithm shall be implicitly known by the receiving party. In this case the asymmetric algorithm shall be defined in the interchange agreement.

The party acting as security originator shall compute a digital signature that shall be conveyed in the USR segment of the security trailer segment group. The party acting as security recipient shall verify the digital signature value.

This service provides also content integrity and origin authentication services.

5.3 Internal representation and filters for compliance with EDIFACT syntax

The use of mathematical algorithms to compute integrity values and digital signatures introduces two problems.

The first problem is that the result of the calculation depends on the internal representation of the character set. Thus the computation of the digital signature by the sender and its verification by the recipient shall be executed using the same character set encoding. Therefore the sender may indicate the representation used to produce the original security validation result.

The second problem is that the result of the calculation is a seemingly random bit pattern. This may cause problems during transmission and with interpretation software. To avoid these problems the bit pattern may be reversibly mapped on to a particular representation of the character set used by means of a filtering function. For simplicity, only one filtering function shall be used for each security service. Any appearance of an anomalous terminator in the output of this mapping is dealt with by including an escape sequence.