INTERNATIONAL STANDARD

ISO 9735-5

First edition
1999-04-01

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

Part 5:

Security rules for batch EDI (authenticity, integrity and non-repudiation of origin)

Échange de données informatisées pour l'administration, le commerce et le transport (EDIFACT) — Règles de syntaxe au niveau de l'application (Numéro de version de syntaxe: 4) —
Partie 5: Règles de sécurité pour EDI par lots (authenticité, intégrité et non-répudiation de l'origine)

Contents

Page

International Organization for Standardization
Case postale 56 • CH-1211 Genève 20 • Switzerland
Internet iso@iso.ch

Printed in Switzerland

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.

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.

This part of ISO 9735 was prepared by the UN/ECE Trade Division (as UN/EDIFACT) and was adopted, under a special "fast-track procedure", by Technical Committee ISO/TC 154, *Documents and data elements in administration, commerce and industry.*

Whereas this part supersedes the earlier publications, and shall use a version number of "4" in the mandatory data element 0002 (Syntax version number) 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 (amended and reprinted in 1990) plus Amendment 1:1992 — *Syntax version number: 3*

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)*:

— *Part 1: Syntax rules common to all parts, together with the syntax service directories for each of the 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)*

Further parts may be added in the future.

Annexes A and B form an integral part of this part of 9735. Annexes C to I 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.

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 securing batch EDIFACT structures i.e. messages, packages, groups or interchange.

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

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

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 part of ISO 9735 shall include conformance to Part 1, Part 2 and Part 8 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 standards contain provisions which, through reference in this text, constitute provisions of this part of ISO 9735. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this part of ISO 9735 are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.

ISO 7498-2:1989, *Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security architecture.*

ISO/IEC 9594-8:1995, *Information technology — Open Systems Interconnection — The Directory: Authentication framework.*

ISO 9735-1:1998, *Electronic data interchange for administration, commerce and transport (EDIFACT) — Application level syntax rules (Syntax version number: 4) — Part 1: Syntax rules common to all parts, together with syntax directories for each of the parts.*

ISO 9735-2:1998, *Electronic data interchange for administration, commerce and transport (EDIFACT) — Application level syntax rules (Syntax version number: 4) — Part 2: Syntax rules specific to batch EDI.*

ISO 9735-6:1998, *Electronic data interchange for administration, commerce and transport (EDIFACT) — Application level syntax rules (Syntax version number: 4) — Part 6: Secure authentication and acknowledgement message (message type — AUTACK).*

ISO 9735-7:—[1)], *Electronic data interchange for administration, commerce and transport (EDIFACT) — Application level syntax rules (Syntax version number: 4) — Part 7: Security rules for batch EDI (confidentiality).*

ISO 9735-8:1998, *Electronic data interchange for administration, commerce and transport (EDIFACT) — Application level syntax rules (Syntax version number: 4) — Part 8: Associated data in EDI.*

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 Definitions

For the purposes of this part of ISO 9735, the definitions in ISO 9735-1:1998, annex A 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

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

This section 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.

1) To be published.

5.1.1 Security header and trailer segment groups

Figure 1 describes an interchange showing security at message level.

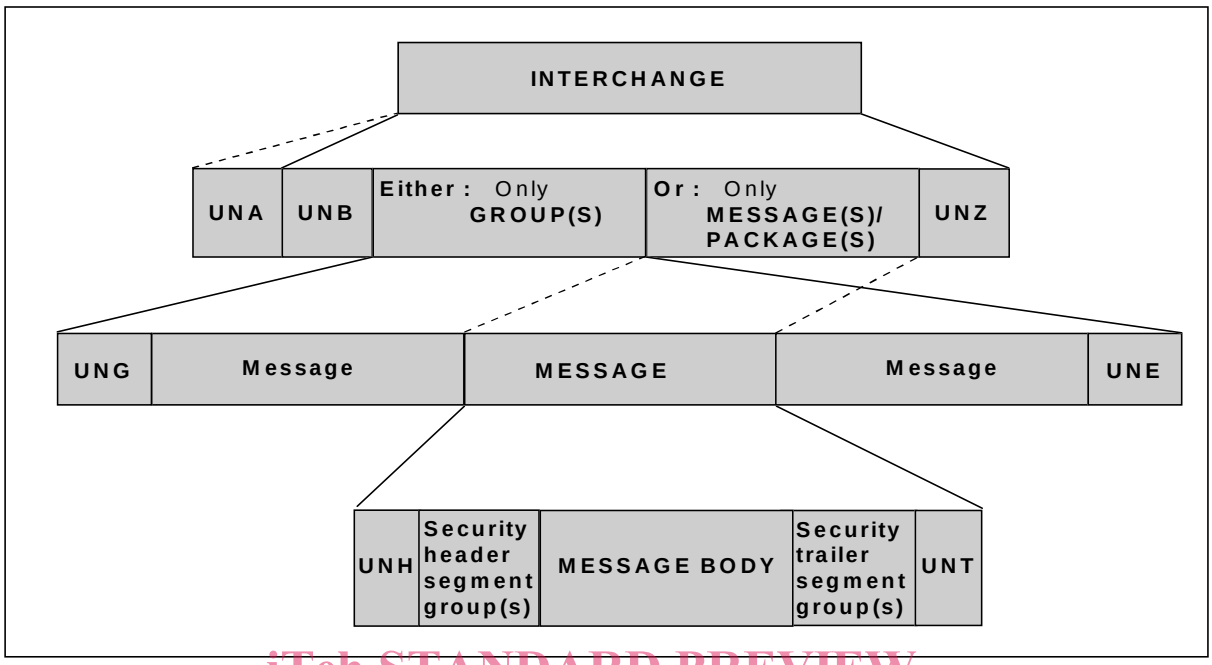

Figure 1 - Interchange showing security at message level (schematic)

Figure 2 describes an interchange showing security at package level.

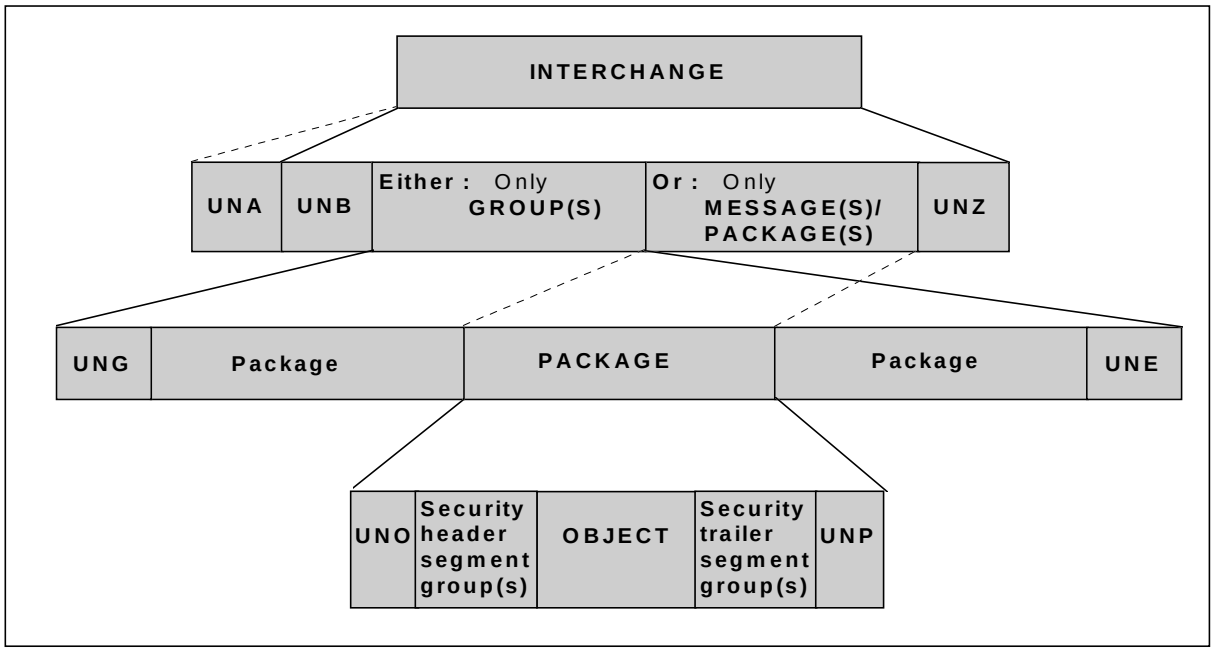

Figure 2 - Interchange showing security at package level (schematic)

5.1.2 Security header and trailer segment groups structure

```
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 1 - Security header and security trailer segment groups segment table (message 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
```


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

Note: UNH message header, UNT message trailer, UNO object header and UNP object trailer are specified in Part 1 of ISO 9735. They are not described further in this Part.

The complete directory specification of the segments and data elements may be found in annex B.

5.1.3 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 Part 7 of ISO 9735.
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 containedin 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

5.1.4 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 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 sub-product 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 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 sub-product 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 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.

6 Rules for the use of interchange and group security header and trailer segment groups for batch EDI

6.1 Group and interchange level security - integrated message security

The security threats relevant to message/package transmission and the security services which address them, as described in annexes C and D, are also valid at group and interchange level.

The techniques described in the previous section for applying security to messages/packages may also be applied to interchanges and groups.

For group and interchange level security, the same header and trailer segment groups as those described at message/package level, shall be used, and header-trailer cross referencing shall always apply at the same level, even when security is applied separately at more than one level.

When security is applied at message/package level, the protected structure is the message body or object. At group level it is the set of messages/packages in the group including all message/package headers and trailers. At interchange level, it is the set of messages/packages or groups in the interchange, including all message/package or group headers and trailers.

6.1.1 Security header and trailer segment groups

Figure 5 describes an interchange showing security at both interchange and group levels.

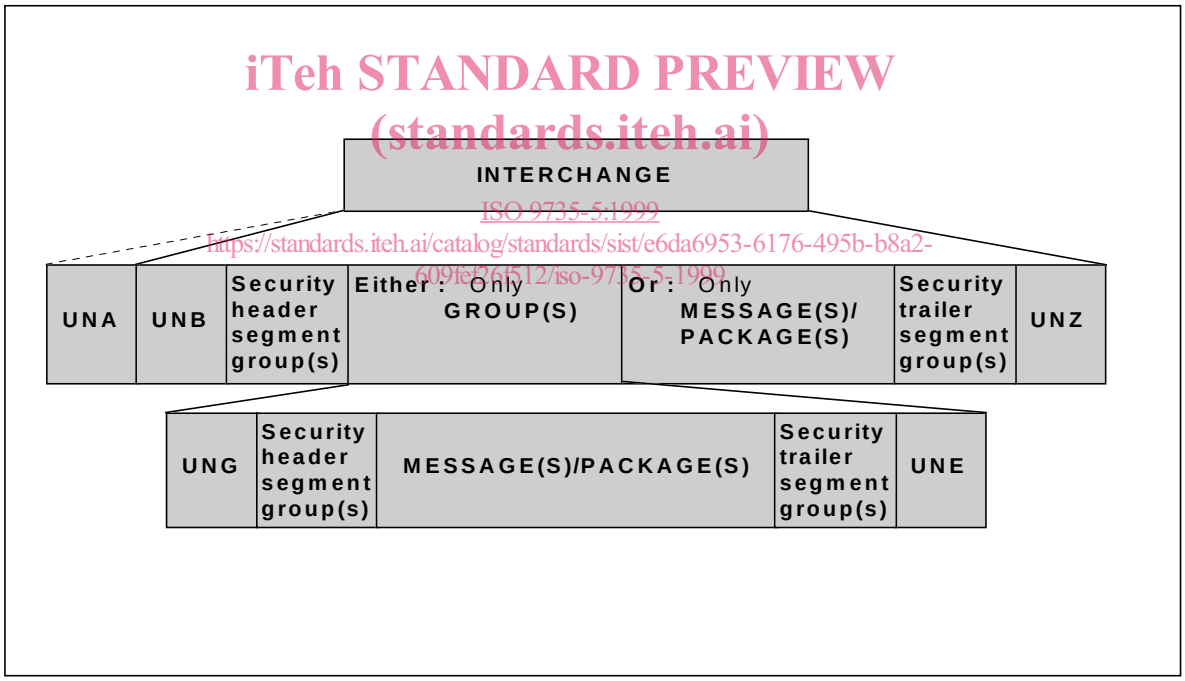

Figure 5 - Interchange showing security at both interchange and group levels (schematic)

6.1.2 Security header and trailer segment groups structure

```
TAG    Name                              S   R

UNB    Interchange 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   --------+
```