INTERNATIONAL STANDARD

ISO 9735-5

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

Échange de données informatisé pour l'administration, le commerce et le transport (EDIFACT) — Règles de syntaxe au niveau de l'application (Numéro de version de syntaxe: 4, numéro d'édition de syntaxe: 1) —

Partie 5: Règles de sécurité pour EDI par lots (authenticité, intégrité et non-répudiation de l'origine)

Reference number
ISO 9735-5:2002(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.ch
Web www.iso.ch

Printed in Switzerland

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 9735-5 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 9735-5:1999). 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 9735-5.

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 E 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.

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, 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.

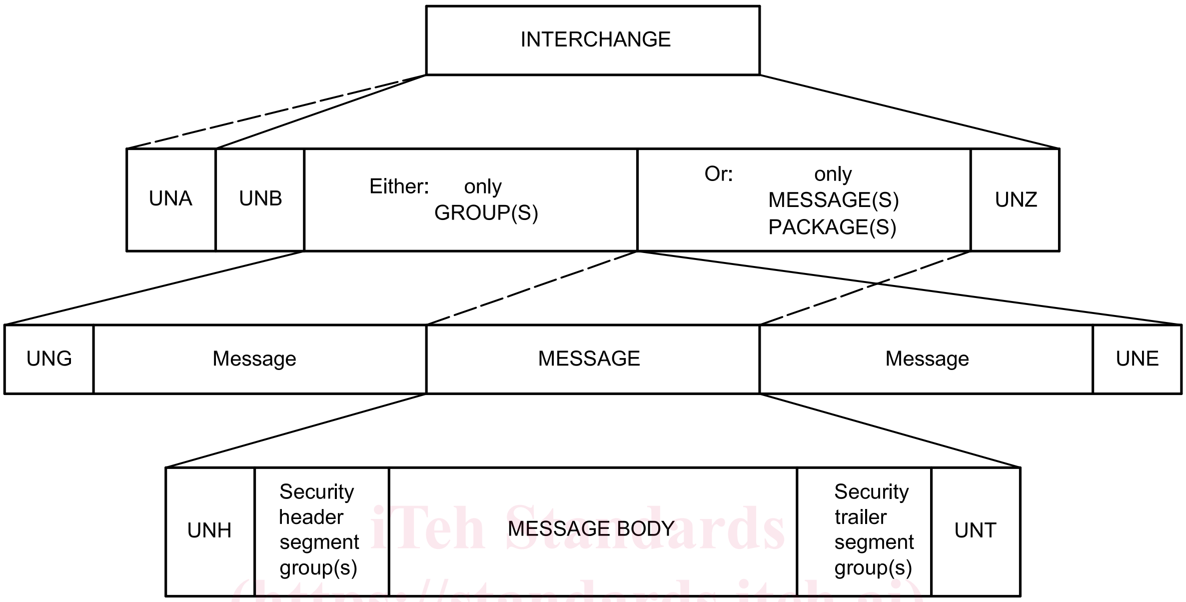

Figure 1 — Interchange showing security at message level (schematic)

Figure 2 describes an interchange showing security at package level.

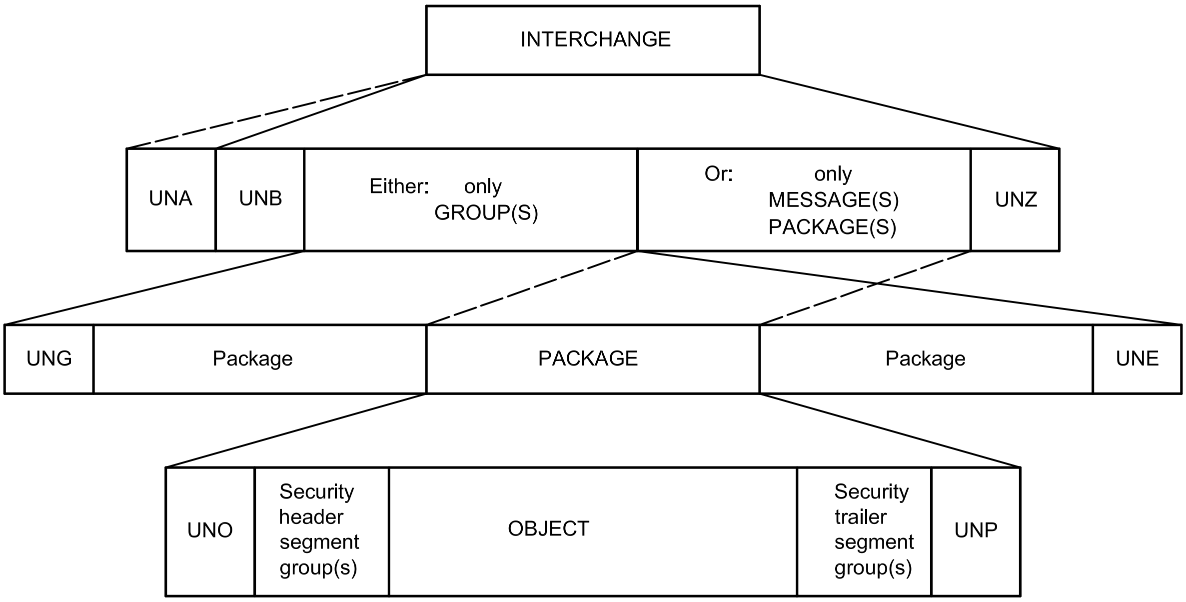

Figure 2 — Interchange showing security at package level (schematic)

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).