INTERNATIONAL STANDARD

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)

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 7: Règles de sécurité pour l'EDI par lots (confidentialité)

Reference number
ISO 9735-7:2002(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 iv
Introduction vi
1 Scope 1
2 Conformance 1
3 Normative references 2
4 Terms and definitions 2
5 Rules for batch EDI confidentiality 2
Annex A (informative) **Message protection example** 10
Annex B (informative) **Processing example** 12
Annex C (informative) **Confidentiality service and algorithms** 14

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.

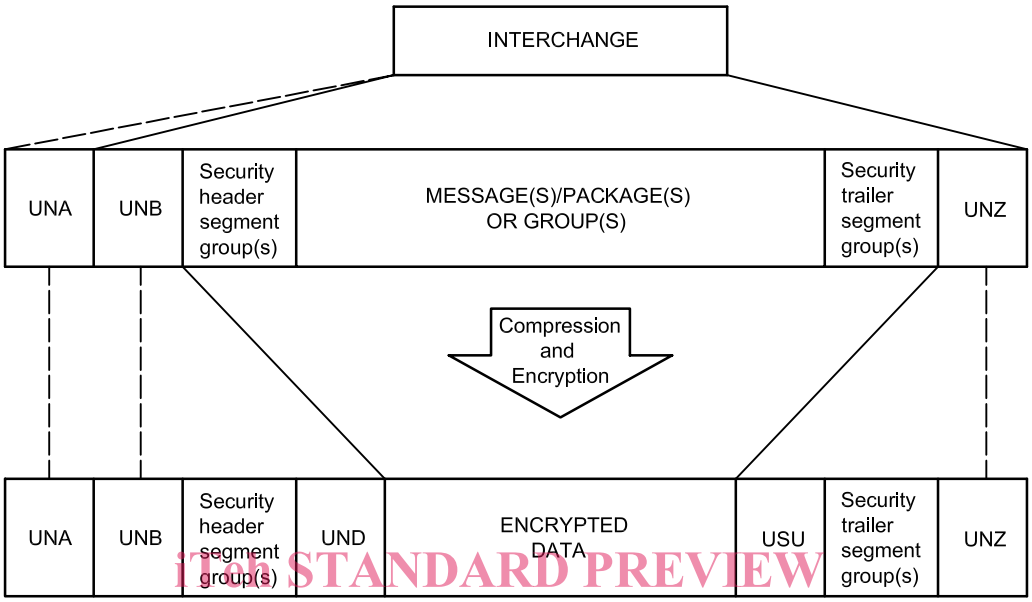

Figure 1 — Structure of an interchange whose contents [message(s)/package(s) or group(s)] have been encrypted (schematic)

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.

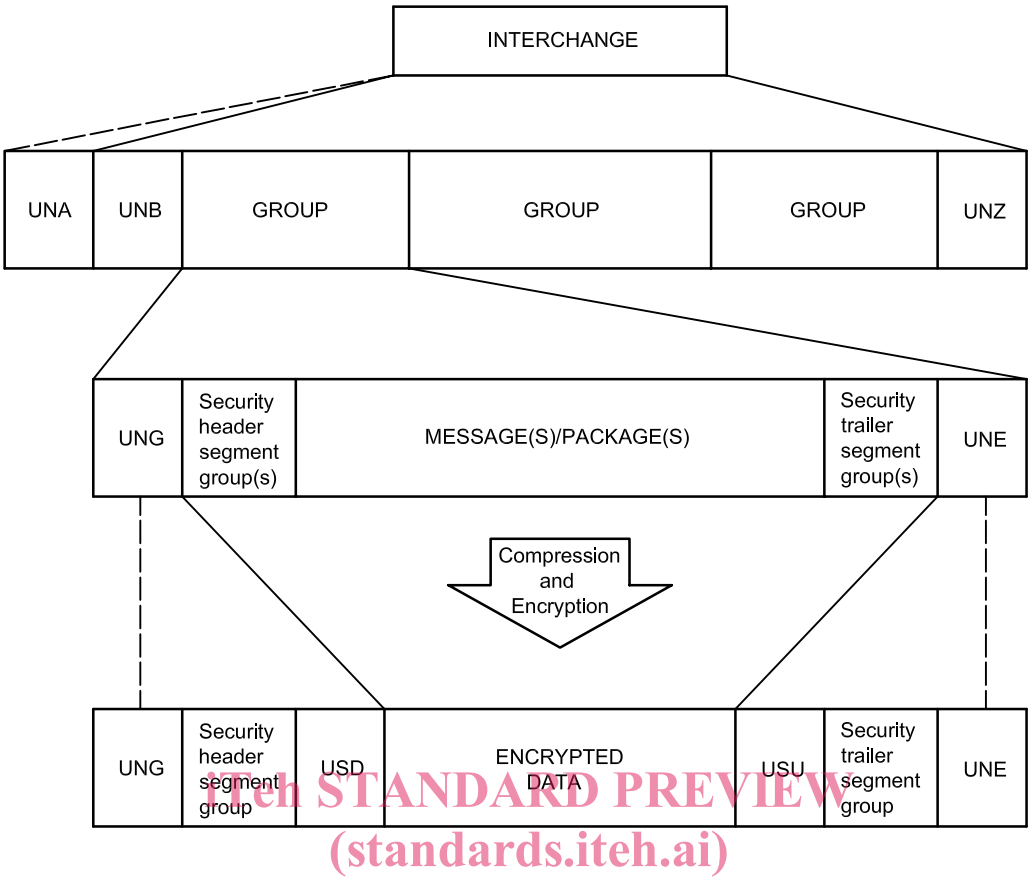

Figure 2 — Structure of an interchange containing one group whose contents (group body and associated security header and trailer segment groups) have been encrypted (schematic)

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.

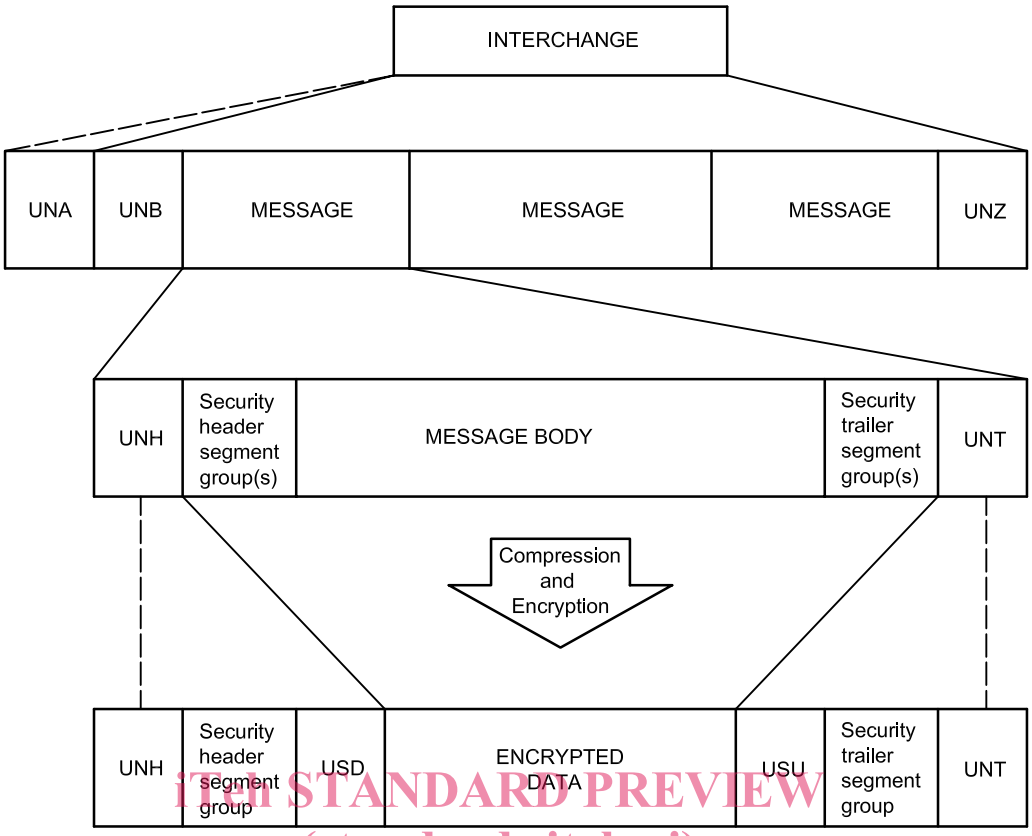

Figure 3 — Structure of an interchange containing one message whose contents (message body and associated security header and trailer segment groups) have been encrypted (schematic)

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.