

Australian Standard™

**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**



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 Standards may also be withdrawn.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 03045.

Australian Standard™

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

First published as AS ISO 9735.7—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 5206 3

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 9735-7:2002, *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)*.

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 7 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

Part 6: Secure authentication and acknowledgement message—message type—AUTACK

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

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:

<i>Reference to International Standard</i>		<i>Australian Standard</i>	
ISO		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	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	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
9735-5	Part 5: Security rules for batch EDI (authenticity, integrity and non-repudiation of origin)	9735.5	Part 5: Syntax rules specific to interactive EDI—authenticity, integrity and non-repudiation of origin
9735-10	Part 10: Syntax service directories	9735.10	Part 10: Syntax service directories

CONTENTS

	<i>Page</i>
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

AUSTRALIAN STANDARD

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.

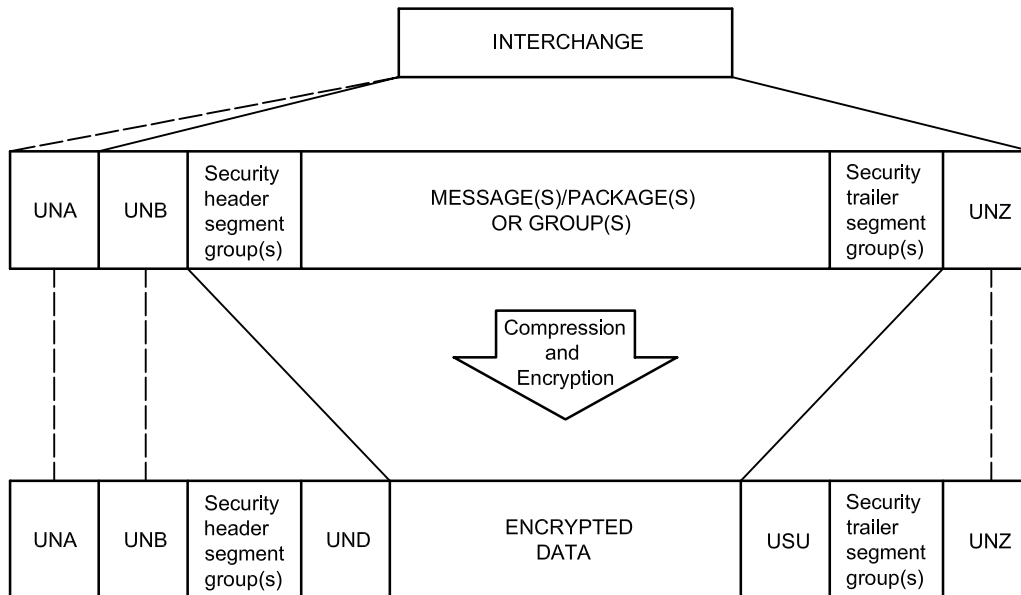


Figure 1 — Structure of an interchange whose contents [message(s)/package(s) or group(s)] have been encrypted (schematic)

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.