

Australian Standard™

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

**Part 9: Security key and certificate
management message—message type—
KEYMAN**



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 Standards may also be withdrawn.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 03047.

Australian Standard™

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

**Part 9: Security key and certificate
management message—message type—
KEYMAN**

First published as AS ISO 9735.9—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 5208 X

 **Documents**
Document Sharing Hub

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 9735-9:2002, *Electronic data interchange for administration, commerce and transport (EDIFACT)—Application level syntax rules (Syntax version number: 4, Syntax release number: 1)—Part 9: Security key and certificate management message (message type—KEYMAN)*.

The objective of this Standard is to define the security key and certificate management message KEYMAN.

This Standard is Part 9 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

Part 8: Associated data in EDI

Part 9: Security key and certificate management message—message type—KEYMAN (this Standard)

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: Security rules for batch EDI—authenticity, integrity and non-repudiation of origin
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 key and certificate management message	2
Annex A	(informative) KEYMAN functions	7
Annex B	(informative) Security techniques to be applied to KEYMAN messages.....	11
Annex C	(informative) Use of segment groups in KEYMAN messages	12
Annex D	(informative) A model for key management.....	14
Annex E	(informative) Key and certificate management examples	16

AUSTRALIAN STANDARD

Electronic data interchange for administration, commerce and transport (EDIFACT) — Application level syntax rules (Syntax version number: 4, Syntax release number: 1) —**Part 9:****Security key and certificate management message (message type — KEYMAN)****1 Scope**

This part of ISO 9735 for batch EDIFACT security defines the security key and certificate management message KEYMAN.

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, 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*

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 key and certificate management message

5.1 Functional definition

KEYMAN is a message providing for security key and certificate management. A key may be a secret key used with symmetric algorithms, or a public or private key used with asymmetric algorithms.

5.2 Field of application

The security key and certificate management message (KEYMAN) may be used for both national and international trade. It is based on universal practice related to administration, commerce and transport, and is not dependent on the type of business or industry.

5.3 Principles

The message may be used to request or deliver security keys, certificates, or certification paths (this includes requesting other key and certificate management actions, for example renewing, replacing or revoking certificates, and delivering other information, such as certificate status), and it may be used to deliver lists of certificates (for example to indicate which certificates have been revoked). The KEYMAN message may be secured by the use of security header and trailer segment groups. Security header and trailer segment group structures are defined in ISO 9735-5.

A security key and certificate management message can be used to:

- a) request actions in relation to keys and certificates;
- b) deliver keys, certificates, and related information.

5.4 Message definition

5.4.1 Data segment clarification

0010 UNH, Message header

A service segment starting and uniquely identifying a message.

The message type code for the security key and certificate management message is KEYMAN.

Security key and certificate management messages conforming to this document must contain the following data in segment UNH, composite S009:

Data element	0065	KEYMAN
	0052	4
	0054	1
	0051	UN

0020 Segment group 1: USE-USX- SG2

A group of segments containing all information necessary to carry key, certificate or certification path management requests, deliveries and notices.

0030 USE, Security message relation

A segment identifying a relationship to an earlier message, such as a KEYMAN request.

0040 USX, Security references

A segment identifying a link to an earlier message, such as a request. The composite data element "security date and time" may contain the original generation date and time of the referenced message.

0050 Segment group 2: USF-USA-SG3

A group of segments containing a single key, single certificate, or group of certificates forming a certification path.

0060 USF, Key management function

A segment identifying the function of the group it triggers, either a request or a delivery. When used for indicating elements of the certification paths, the certificate sequence number shall indicate the position of the following certificate within the certification path. It may be used on its own for list retrieval, with no certificate present. There may be several different USF segments within the same message, if more than one key or certificate is handled. However, there shall be no mixture of request functions and delivery functions. The USF segment may also specify the filter function used for binary fields of the USA segment immediately following this segment.

0070 USA, Security algorithm

A segment identifying a security algorithm, the technical usage made of it, and containing the technical parameters required (as defined in ISO 9735-5). This segment shall be used for symmetric key requests, discontinuation or delivery. It may also be used for an asymmetric key pair request.

0080 Segment group 3: USC-USA-USR

A group of segments containing the data necessary to validate the security methods applied to the message/package, when asymmetric algorithms are used (as defined in ISO 9735-5). This group shall be used in the request or delivery of keys and certificates.

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 desired 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

0090 USC, Certificate

A segment containing the credentials of the certificate owner and identifying the certification authority which has generated the certificate (as defined in ISO 9735-5). This segment shall be used for certificate requests such as renewal, or asymmetric key requests such as discontinuation, and for certificate deliveries.

0100 USA, Security algorithm

A segment identifying a security algorithm, the technical usage made of it, and containing the technical parameters required (as defined in ISO 9735-5). This segment shall be used for certificate requests such as credentials registration, and for certificate deliveries.

0110 USR, Security result

A segment containing the result of the security functions applied to the certificate by the certification authority (as defined in ISO 9735-5). This segment shall be used for certificate validation or certificate deliveries.

0120 Segment group 4: USL-SG5

A group of segments containing lists of certificates or public keys. The group shall be used to group together certificates of similar status — i.e. which are still valid, or which may be invalid for some reason.

0130 USL, Security list status

A segment identifying valid, revoked, unknown or discontinued items. These items may be certificates (e.g. valid, revoked) or public keys (e.g. valid or discontinued). There may be several different USL segments within this message, if the delivery implies more than one list of certificates or public keys. The different lists may be identified by the list parameters.

0140 Segment group 5: USC-USA-USR

A group of segments containing the data necessary to validate the security methods applied to the message/package, when asymmetric algorithms are used (as defined in ISO 9735-5). This group shall be used in the delivery of lists of keys or certificates of similar status.

0150 USC, Certificate

A segment containing the credentials of the certificate owner and identifying the certification authority which has generated the certificate (as defined in ISO 9735-5). This segment shall be used either in the full certificate using in addition the USA and USR segments, or may alternatively indicate the certificate reference number or key name, in which case the message shall be signed using security header and trailer segment groups.

0160 USA, Security algorithm

A segment identifying a security algorithm, the technical usage made of it, and containing the technical parameters required (as defined in ISO 9735-5). If it is required to indicate the algorithms used with a certificate, this segment shall be used.