AS ISO 9735.9—2003
ISO 9735-9:2002

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

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 Standards may also be withdrawn.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.

Published by Standards Australia International Ltd
GPO Box 5420, Sydney, NSW 2001, Australia

ISBN 0 7337 5208 X

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:

Reference to International Standard		*Australian Standard*	
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.