
**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)**

ISO 9735-9:2002

<https://standards.iso.org/standards.html> *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 9: Clé de sécurité et message de gestion de certificat (type de message KEYMAN)



PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO 9735-9:2002

<https://standards.iteh.ai/catalog/standards/sist/79a6cd85-0efa-4128-8e7d-d3a01a906c37/iso-9735-9-2002>

© ISO 2002

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

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 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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO 9735-9:2002

<https://standards.iteh.ai/catalog/standards/sist/79a6cd85-0efa-4128-8e7d-d3a01a906c37/iso-9735-9-2002>

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 9735-9 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 9735-9:1999). 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 9735-9.

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO 9735-9:2002

<https://standards.iteh.ai/catalog/standards/sist/79a6cd85-0efa-4128-8e7d-d3a01a906c37/iso-9735-9-2002>

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 batch 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 managing security keys and certificates.

iTeh STANDARD PREVIEW (standards.iteh.ai)

ISO 9735-9:2002

<https://standards.iteh.ai/catalog/standards/sist/79a6cd85-0efa-4128-8e7d-d3a01a906c37/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)

1 Scope

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

2 Conformance

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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.

0170 **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). If it is required to sign a certificate, this segment shall be used.

0180 **UNT, Message trailer**

A service segment ending a message, giving the total number of segments and the control reference number of the message.

5.4.2 Data segment index**TAG Name**

UNH Message header

UNT Message trailer

USA Security algorithm

USC Certificate

USE Security message relation

USF Key management function

USL Security list status

USR Security result

USX Security references

ITEH STANDARD PREVIEW
(standards.iteh.ai)

ISO 9735-9:2002

standards.iteh.ai/catalog/standards/sist/79a6cd85-0efa-4128-8e7d-d3a01a906c37/iso-9735-9-2002

5.4.3 Message structure

Table 1 — Segment table

POS	TAG	Name	S	R	
0010	UNH	Message header	M	1	
0020	-----	Segment group 1 -----	C	999	-----+
0030	USE	Security message relation	M	1	
0040	USX	Security references	C	1	
0050	-----	Segment group 2 -----	M	9	-----+
0060	USF	Key management function	M	1	
0070	USA	Security algorithm	C	1	
0080	-----	Segment group 3 -----	C	1	---+
0090	USC	Certificate	M	1	
0100	USA	Security algorithm	C	3	
0110	USR	Security result	C	1	-----+
0120	-----	Segment group 4 -----	C	99	-----+
0130	USL	Security list status	M	1	
0140	-----	Segment group 5 -----	M	9999	-----+
0150	USC	Certificate	M	1	
0160	USA	Security algorithm	C	3	
0170	USR	Security result	C	1	-----+
0180	UNT	Message trailer	M	1	

ISO 9735-9:2002

<https://standards.iteh.ai/catalog/standards/sist/79a6cd85-0efa-4128-8e7d-d3a01a906c37/iso-9735-9-2002>