INTERNATIONAL STANDARD

ISO 9735-9

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

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)

Reference number
ISO 9735-9:2002(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

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.

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.

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.

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

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	

Annex A
(informative)

KEYMAN functions

A.1 Introduction

This annex describes the different functions provided by KEYMAN. In the following, credentials will just mean information relating to one particular party, but not the public key, nor timestamps. So a certificate will consist of

— credentials;

— a public key;

— timestamps;

— a digital signature.

Certain functions are considered to be handled out of band, i.e. using a communication channel different from that normally used. This is the case with communication of the secret key of the user, if he is not responsible for his own key generation.

A.2 Registration-related key management functions

A.2.1 Registration submission

The purpose is to submit (part of) certificate content for registration.

Although this function typically will be backed up by some secure out of band technique (such as a personal visit, or a human signature), it may be more efficient for the registration authority (RA, an authority trusted by one or more users to register users) not to have to re-key the information, but merely to check it. For this reason, this message itself need not be secured, though integrity checking using the normal header/trailer approach defined in ISO 9735-5 may be useful, if further secured out of band.

A.2.2 Asymmetric key pair request

The purpose is to request a trusted party to generate an asymmetric key pair. The subsequent transport of the secret key must be handled out of band.

A.3 Certification-related key management functions

A.3.1 Certification request

The purpose is to request certification of credentials and public key.

It may be presumed to be merely a request following prior out of band transfer of information, in which case the request itself results in no transfer of information. No registered keys may yet available, so it is assumed to be an unsecured message. However, if this information is transmitted in the message, it will require separate authentication. If a registered key already exists, then this may be used to provided non-repudiation of origin for the information for the new key and certificate.

Nevertheless, if the message is used by a user to forward his public key, it should be possible for him to sign it with the corresponding secret key, even though no label exists yet for the public key. This is called self-certification, and requires the use of security header and trailer segment groups. To indicate that the key is self-certified, the security header segment group defined in ISO 9735-5 must contain a certificate issued by the user on his own key. Although a self-certified public key does not prove its user's authenticity to another party, it does prove to the certification authority that the user is in possession of the corresponding private key.

A.3.2 Certificate renewal request

The purpose is to request the renewal (or update) of a certificate.

The purpose of this is to extend the validity period of the current valid key, whose certificate is about to expire. The request must be signed, using EDIFACT security header and trailer segment groups described in ISO 9735-5, by the private key certified by the certificate to be renewed.

A.3.3 Certificate replacement request

The purpose is to request the replacement of a current certificate by a new one with a different public key, as well as giving additional information if required. The request must be signed according to an agreed policy using EDIFACT header and trailer segment groups described in ISO 9735-5.

It differs from a renewal request in that the old certificate typically is revoked, rather than expiring. A new certificate always has a new certificate reference number, while a revocation certificate always carries the same reference number as the certificate being revoked.

A.3.4 Certificate (path) retrieval request

The purpose is to request the delivery of an existing certificate, valid or a revoked, or a revocation certificate. This also includes the situation where the response contains a certification path rather than just a certificate, as usually the inquirer is ignorant to such details.

If the certificate reference number has been specified, there are no requirements for security since the certificates are public.

A.3.5 Certificate delivery

The purpose is to deliver an existing certificate or revocation certificate with or without prior request.

The certification authority (CA) public key transport would normally be handled out of band. However, for convenience of re-keying, a message may be required, possibly secured by header and trailer segment groups for integrity, with separate authentication. If available, it may tempt users to ignore checking the out of band value, in which case it will actually reduce security considerably. This may require security services, such as non-repudiation of origin.

A.3.6 Certificate status request

The purpose is to request the current status of a given certificate.

A.3.7 Certificate status notice

The purpose is to inform the requesting party about the status of the given certificate.

The possible status's are: unknown, valid or revoked. This notice may be delivered without prior request and would typically have to be secured by non-repudiation of origin.

A.3.8 Certificate validation request

The request is to be forwarded to a CA for the validation of an existing certificate.

This pertains to certificates of other security domains (i.e. issued by other CA's), in which case the user may be unable to establish the validity.

A.3.9 Certificate validation notice

This is the response to a certificate validation request. It is recommended to use non-repudiation of origin or other means of authentication for this.

A.4 Revocation-related key management functions

A.4.1 Revocation request

The purpose is to request revocation (the change of status from valid to invalid) of a party's certificate, e.g. because the private key has been compromised, the user has changed to a new CA, the original certificate has been superseded, use has been terminated (for example, the user left the company), or some other reason. It is recommended to use authentication if possible. The function may require a separate channel, and may cover the case where the user has lost the private key.

A.4.2 Revocation confirmation

The purpose is to confirm the revocation of the requested certificate.

It is recommended to secure this by means of non-repudiation of origin.

A.4.3 Revocation list request

The purpose is to request full or partial list of revoked certificates.

A.4.4 Revocation list delivery

The purpose is to inform parties about all (or a specified subset of all) currently revoked certificates in the CA's domain.

This is like a multiple status notice, but only for revoked certificates. While it would be possible to have a separate black list type, it is probably better to just have one, and identify the status. The delivery should be secured by non-repudiation of origin.

A.5 Alert request

The purpose is to request a party's certificate to be put on alert.

The certificate is not revoked (no request to the CA) but the other users are warned that there can be something wrong with this certificate. This could be used if no appropriate means of authentication is available to secure a revocation request, for example a second, valid, key and certificate.

A.6 Certificate path delivery

The purpose is to deliver an existing certification path with or without prior request.

A.7 Symmetric key generation and transport

A.7.1 Symmetric key request

The purpose is to request the delivery of symmetric data keys or key encryption keys. Since the delivery of the keys implies a prior secure relationship between the two parties, the originator must be authenticated using a key encrypting key (KEK, a key used to provide confidentiality for another key), if public key techniques are not used.

A.7.2 Symmetric key delivery

The purpose is to deliver symmetric keys (with or without prior request).

If symmetric techniques are used only, it must be assumed that an out of band transfer of a KEK would be necessary before the transfer. The algorithm parameter in USA would then carry the encrypted key.

A.8 Key discontinuation

A.8.1 (A)symmetric key discontinuation request

The purpose is to request discontinuation of an existing symmetric or asymmetric key (if certificates are not used), e.g. because the key has been compromised, the original key has been superseded, use has been terminated (for example the user left the company), or some other reason. It is recommended to secure this using existing keys for authentication.

A.8.2 Discontinuation acknowledgement

The purpose is to confirm that some specified key(s) has been discontinued.

Remark: Functions that can not be supported by a KEYMAN message:

— Independent time-stamping functions (require a separate message, e.g. AUTACK).

— Acknowledgement and error notification related to received KEYMAN messages will require the use of other messages, e.g. AUTACK or CONTRL.

Annex B
(informative)

Security techniques to be applied to KEYMAN messages

This annex suggests the minimum and maximum level of header/trailer (H/T) security, as described in ISO 9735-5, to be used with each KEYMAN function.

Table B.1 — Levels of header/trailer (H/T) security

Function	H/T Security		Comments
	MIN	MAX	
Registration submission		INT	Out of band AUT
Asymmetric key pair request			
Certification request		NRO	Out of band AUT
Certificate renewal request	NRO		
Certificate replacement request	NRO		
Certificate (path) retrieval request		NRO	
Certificate delivery			
Certificate status request		NRO	
Certificate status notice		NRO	
Certificate validation request			
Certificate validation notice	NRO		
Revocation request	NRO		
Revocation confirmation	NRO		
Revocation list request			
Revocation list delivery	NRO		
Alert request		NRO	
Certificate path delivery			
Symmetric key request			
Symmetric key delivery	CON		May use KEK
(A)symmetric key discontinuation request	AUT	NRO	
Discontinuation acknowledgement	AUT	NRO	

Key

AUT	Authentication
CON	Confidentiality
INT	Integrity
KEK	Key encrypting key
NRO	Non-repudiation of origin
Out of band	Using a communication channel different from that normally used

Annex C
(informative)

Use of segment groups in KEYMAN messages

This annex describes which segment groups are used to provide particular KEYMAN functions.

Table C.1 — Segment groups for requests

Function	Segments	Comments
Registration submission	USE-USF-USC-USA	
Asymmetric key pair request	USE-USF-USA	
Certification request	USE-USF-USC-USA	Identify the certificate and public key.
Certificate renewal request	USE-USF-USC	Identify the certificate and specify the new validity period.
Certificate replacement request	USE-USF-USC-USA	The current certificate to be revoked is referred in a similar group.
Certificate (path) retrieval request	USE-USF-USC	Certificate list retrieval is included here, using USF.
Certificate status request	USE-USF-USC	
Certificate validation request	USE-USF-USC-USA(3)-USR	
Revocation request	USE-USF-USC	Out of band as well.
Revocation list request	USE-USF	
Alert request	USE-USF-USC	
Symmetric key request	USE-USF-USA	Symmetric only. USA defines the key name if required.
(A)symmetric key discontinuation request	USE-USF-USA/USC	Sym/Asym. Identify the keys.
Key Out of band Using a communication channel different from that normally used.		

Table C.2 — Segment groups for deliveries or notices

Function	Segments	Comments
Certificate delivery	USE-USX-USF-USC-USA(3)-USR	
Certificate status notice	USE-USX-USF-USC-USA(3)-USR	May be like certificate/path delivery: revocation reason is added to the normal certificate, and/or the status is obvious from USF.
Certificate validation notice	USE-USX-USF-USC-USA(3)-USR	Like certificate status notice, secured by NRO.
Revocation confirmation	USE-USX-USF-USC	Like certificate status notice. Must be secured by NRO.
Revocation list delivery	USL-USC	Like multiple certificate status notice, but only for revoked certificates.
Certificate path delivery	USE-USX-USF-USC-USA(3)-USR	Repeat USF group for paths.
Symmetric key delivery	USE-USX-USF-USA	Symmetric only. An out of band transfer of a KEK is necessary before.
Discontinuation acknowledgement	USE-USX-USF-USA/USC	Sym/Asym. Like certificate status notice. Must be secured by authentication/NRO.

Key

KEK	Key encrypting key.
NRO	Non-repudiation of origin.
Out of band	Using a communication channel different from that normally used.

Annex D
(informative)

A model for key management

D.1 Introduction

Key management deals with the generation, distribution, certification, verification and revocation of cryptographic keys in an open and secure information system. The model considered here is depicted in Figure D.1, where five logical parties are defined according to their functionality.

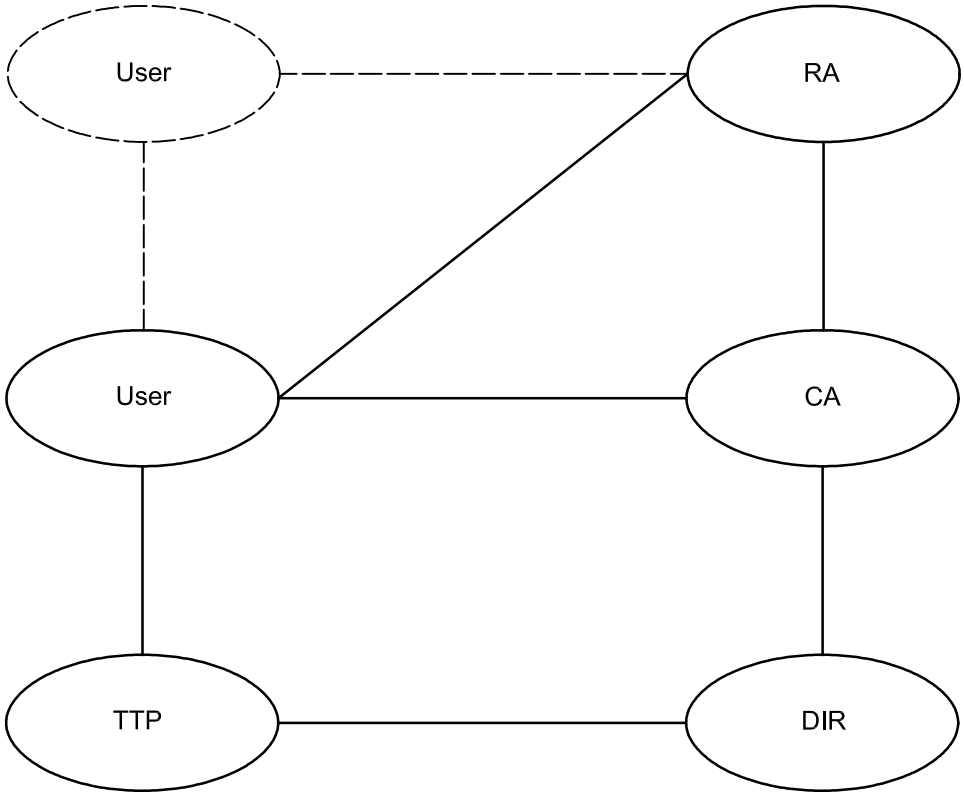

Figure D.1 — Key management model

The basic assumption of this model is that public key techniques for security services are used. Moreover, the architecture is according to the ITU/TS X.509 framework standard.

A security domain is defined as the “jurisdiction” of the pair of public keys used by the certification authority (CA) to issue certificates. Thus there is only one CA within a security domain, and the security domain is characterized by the fact that all users of that domain are certified with the same secret key under the control of the CA.

The CA is connected by means of secured communication to a number of registration authorities (RA), through which any user may register. A registration is acknowledged by a certificate issued by the CA at the request of some RA. Furthermore public information on the users, such as certificates is available in a directory (DIR). Finally, a number of additional trusted third parties (TTP’s) may register as well as users offering special services.

D.2 The end-user (U)

By a user (U) is meant the unique user-Id in the system, as identified by his credentials. A real user may have more than one Id. In fact, a user-Id may represent a legal person, a real, (or moral), person or a system device.

D.3 The registration authority (RA)

For an unregistered user, there is no established electronic security link between the user and the system. RA is used as an entry point for users to set-up such links by using some existing trusted means such as registered letters or personal enrolment. This registration will also form the legal basis for the use of digital signatures by the user, if required, although this aspect in itself is not key management. Once this registration has been established, the user credentials and his public key are passed on the CA with a request for certification.

D.4 The certification authority (CA)

The certification authority is the central party of the system. It provides certificates to the users so that “trust” can be established between different users based on the “trust” between the RA’s and users. These certificates are furthermore made available in one or more directories which can be accessed by all users.

It is a common misunderstanding that the fact that a certificate has been issued implies that one can trust the public key to be valid. If a public key is cancelled at a later stage, after the certificate was issued, the certificate is no longer valid. Instead, the CA issues a revocation certificate, which is placed in the directory to replace the original certificate. The users will therefore have to consult the directory at regular intervals for verification even though certificates are used. How often is a question of risk assessment.

D.5 The directory (DIR)

The public directory (DIR), acting like a public telephone book, is responsible for holding the current certificates, as well as revocation certificates, for ready on-line inspection by other users. It is essential, that the communication between users and the DIR is secured in order to guarantee that the information drawn from the DIR is up to date and correct.

In fact, the DIR will typically continuously certify the current status of the CA certificates by means of its own secret key. This in particular requires that the directory is registered as a user with a public key by the CA.

D.6 Trusted third party (TTP) services

A trusted third party is a party which at least two other parties trust. TTP’s may provide some additional services such as time-stamping, etc. The TTP services relevant to EDI include:

— independent time-stamping;

— attribute certificates;

— notary functions;

— document repository;

— non-repudiation of submission/delivery;

— translation/validation of certificates.

Annex E
(informative)

Key and certificate management examples

Four examples are provided herein to illustrate different applications of the KEYMAN message.

E.1 Revocation request

E.1.1 Narrative

A certificate previously issued by certification authority CA2 for an employee E1 of an organization O1 is revoked by the organization because the employee left at midday GMT on 31 December 1996. This message from the organization to the certification authority will be signed for non-repudiation of origin by the organization in the normal way using security header and trailer segment groups as described in ISO 9735-5. The message may be responded to by a revocation confirmation from CA2 to O1.

E.1.2 Security details

SECURITY MESSAGE RELATION	
MESSAGE RELATION	'1' no relation

KEY MANAGEMENT FUNCTION	
KEY MANAGEMENT FUNCTION QUALIFIER	'130' revocation request

CERTIFICATE	
CERTIFICATE REFERENCE	'CA2-O1-E1' (eg) the certificate in question
SECURITY IDENTIFICATION DETAILS	
Security party qualifier	'3' certificate owner
Key name	
Security party identification	'O1-E1' (eg) the employee within the organization
Security party code list qualifier	'ZZZ' mutually agreed
Security party code list responsible agency	'1' UN/CEFACT
SECURITY IDENTIFICATION DETAILS	
Security party qualifier	'4' authenticating party
Key name	
Security party identification	'CA2' the certification authority
Security party code list qualifier	'ZZZ' mutually agreed
Security party code list responsible agency	'1' UN/CEFACT
SECURITY DATE AND TIME	
Date and time qualifier	'6' certificate revocation date and time
Event date	'19961231
Event time	'120000'
Time offset	'0000'
REVOCATION REASON	'3' owner changed affiliation

E.2 Symmetric key discontinuation request

E.2.1 Narrative

Organization O1 requests organization O2 to stop using a mutual symmetric key K1, because it has been superseded. This message between the organizations will be protected for message origin authentication by the organization in the normal way using security header and trailer segment groups as described in ISO 9735-5 using another previously agreed symmetric key. The message may be responded to by a discontinuation acknowledgement from O2 to O1.

E.2.2 Security details

SECURITY MESSAGE RELATION	
MESSAGE RELATION	'1' no relation

KEY MANAGEMENT FUNCTION	
KEY MANAGEMENT FUNCTION QUALIFIER	'151' symmetric key discontinuation request

SECURITY ALGORITHM	
SECURITY ALGORITHM	
Use of algorithm	'2' owner symmetric
Cryptographic mode of operation	'2' CBC
Algorithm	'1' DES
ALGORITHM PARAMETER	
Algorithm parameter qualifier	'9' symmetric key name
Algorithm parameter value	'K1'

E.3 Certificate (path) delivery

E.3.1 Narrative

This message from certification authority CA2 to an organization O1 follows an earlier certificate (path) retrieval request from the organization to their certification authority for the path of organization O2's certificate. In this example CA2 and O2's certification authority, CA3, are both certified by certification authority CA1 in a two level hierarchy. The request message could be referred to explicitly by using the USX segment between the USE and USF segments.

All certificates times are midnight GMT, with the top level certificate being generated on 1 December 1996 for use from 1 January 1997 for 10 years, and the user certificate being generated on 1 February 1997 for use from 1 March 1997 for two years. The CA1, CA3 and O2 public key lengths are 2048, 1024 and 512 respectively. All public key exponents are 10001_{16}.

E.3.2 Security details

SECURITY MESSAGE RELATION	
MESSAGE RELATION	'2' response

KEY MANAGEMENT FUNCTION	
KEY MANAGEMENT FUNCTION QUALIFIER	'222' certificate path delivery
CERTIFICATE SEQUENCE NUMBER	'1' the first certificate in the path

CERTIFICATE	
CERTIFICATE REFERENCE	'CA1-CA3' (eg) CA1's certificate for CA3
SECURITY IDENTIFICATION DETAILS	
Security party qualifier	'3' certificate owner
Key name	
Security party identification	'CA3' O2's certification authority
Security party code list qualifier	'ZZZ' mutually agreed
Security party code list responsible agency	'1' UN/CEFACT
SECURITY IDENTIFICATION DETAILS	
Security party qualifier	'4' authenticating party
Key name	
Security party identification	'CA1' the top level certification authority
Security party code list qualifier	'ZZZ' mutually agreed
Security party code list responsible agency	'1' UN/CEFACT
Certificate Syntax and version	'1' version 4
FILTER FUNCTION	'2' hexadecimal filter
ORIGINAL CHARACTER SET ENCODING	'1' ASCII 7 bit code
CERTIFICATE ORIGINAL CHARACTER SET REPERTOIRE	'2' UN/ECE syntax level B
SERVICE CHARACTER FOR SIGNATURE	
Service character for signature qualifier	'1' segment terminator
Service character for signature	'27' apostrophe
SERVICE CHARACTER FOR SIGNATURE	
Service character for signature qualifier	'2' component data element separator
Service character for signature	'3A' colon
SERVICE CHARACTER FOR SIGNATURE	
Service character for signature qualifier	'3' data element separator
Service character for signature	'2B' plus sign
SERVICE CHARACTER FOR SIGNATURE	
Service character for signature qualifier	'4' release character
Service character for signature	'3F' question mark
SERVICE CHARACTER FOR SIGNATURE	
Service character for signature qualifier	'5' repetition separator
Service character for signature	'2A' asterisk
SECURITY DATE AND TIME	
Date and time qualifier	'2' certificate generation date and time
Event date	'19961201'
Event time	'000000'
Time offset	'0000'
SECURITY DATE AND TIME	
Date and time qualifier	'3' certificate start of validity period
Event date	'19970101'
Event time	'000000'
Time offset	'0000'

SECURITY DATE AND TIME	
Date and time qualifier	'4' certificate end of validity period
Event date	'20070101'
Event time	'000000'
Time offset	'0000'
SECURITY STATUS	'1' valid
SECURITY ALGORITHM	
SECURITY ALGORITHM	
Use of algorithm	'6' owner signing
Cryptographic mode of operation	
Algorithm	'10' RSA
ALGORITHM PARAMETER	
Algorithm parameter qualifier	'13' exponent
Algorithm parameter value	'010001'
ALGORITHM PARAMETER	
Algorithm parameter qualifier	'12' modulus
Algorithm parameter value	CA3's public key
ALGORITHM PARAMETER	
Algorithm parameter qualifier	'14' modulus length
Algorithm parameter value	'1024'

SECURITY ALGORITHM	
SECURITY ALGORITHM	
Use of algorithm	'4' issuer hashing
Cryptographic mode of operation	
Algorithm	'42' HDS2

SECURITY ALGORITHM	
SECURITY ALGORITHM	
Use of algorithm	'3' issuer signing
Cryptographic mode of operation	
Algorithm	'10' RSA
ALGORITHM PARAMETER	
Algorithm parameter qualifier	'13' exponent
Algorithm parameter value	'010001'
ALGORITHM PARAMETER	
Algorithm parameter qualifier	'12' modulus
Algorithm parameter value	CA1's public key
ALGORITHM PARAMETER	
Algorithm parameter qualifier	'14' modulus length
Algorithm parameter value	'2048'

SECURITY RESULT	**Digital signature of the certificate by CA1**
VALIDATION RESULT	
Validation value qualifier	'1' unique validation value
Validation value	the filtered 2048 Bit digital signature

KEY MANAGEMENT FUNCTION	
KEY MANAGEMENT FUNCTION QUALIFIER	'222' certificate path delivery
CERTIFICATE SEQUENCE NUMBER	'2' the second certificate in the path

CERTIFICATE	
CERTIFICATE REFERENCE	'CA3-O2' (eg) CA3's certificate for O2
SECURITY IDENTIFICATION DETAILS	
Security party qualifier	'3' certificate owner
Key name	
Security party identification	'O2' organization O2
Security party code list qualifier	'ZZZ' mutually agreed
Security party code list responsible agency	'1' UN/CEFACT
SECURITY IDENTIFICATION DETAILS	
Security party qualifier	'4' authenticating party
Key name	
Security party identification	'CA3' O2's certification authority
Security party code list qualifier	'ZZZ' mutually agreed
Security party code list responsible agency	'1' UN/CEFACT
Certificate Syntax and version	'1' version 4
FILTER FUNCTION	'2' hexadecimal filter
ORIGINAL CHARACTER SET ENCODING	'1' ASCII 7 bit code
CERTIFICATE ORIGINAL CHARACTER SET REPERTOIRE	'2' UN/ECE syntax level B
SERVICE CHARACTER FOR SIGNATURE	
Service character for signature qualifier	'1' segment terminator
Service character for signature	'27' apostrophe
SERVICE CHARACTER FOR SIGNATURE	
Service character for signature qualifier	'2' component data element separator
Service character for signature	'3A' colon
SERVICE CHARACTER FOR SIGNATURE	
Service character for signature qualifier	'3' data element separator
Service character for signature	'2B' plus sign
SERVICE CHARACTER FOR SIGNATURE	
Service character for signature qualifier	'4' release character
Service character for signature	'3F' question mark
SERVICE CHARACTER FOR SIGNATURE	
Service character for signature qualifier	'5' repetition separator
Service character for signature	'2A' asterisk
SECURITY DATE AND TIME	
Date and time qualifier	'2' certificate generation date and time
Event date	'19970201'
Event time	'000000'
Time offset	'0000'
SECURITY DATE AND TIME	
Date and time qualifier	'3' certificate start of validity period
Event date	'19970301'
Event time	'000000'
Time offset	'0000'

SECURITY DATE AND TIME	
Date and time qualifier	'4' certificate end of validity period
Event date	'19990301'
Event time	'000000'
Time offset	'0000'
SECURITY STATUS	'1' valid

SECURITY ALGORITHM	
SECURITY ALGORITHM	
Use of algorithm	'6' owner signing
Cryptographic mode of operation	
Algorithm	'10' RSA
ALGORITHM PARAMETER	
Algorithm parameter qualifier	'13' exponent
Algorithm parameter value	'010001'
ALGORITHM PARAMETER	
Algorithm parameter qualifier	'12' modulus
Algorithm parameter value	O2's public key
ALGORITHM PARAMETER	
Algorithm parameter qualifier	'14' modulus length
Algorithm parameter value	'512'

SECURITY ALGORITHM	
SECURITY ALGORITHM	
Use of algorithm	'4' issuer hashing
Cryptographic mode of operation	
Algorithm	'42' HDS2

SECURITY ALGORITHM	
SECURITY ALGORITHM	
Use of algorithm	'3' issuer signing
Cryptographic mode of operation	
Algorithm	'10' RSA
ALGORITHM PARAMETER	
Algorithm parameter qualifier	'13' exponent
Algorithm parameter value	'010001'
ALGORITHM PARAMETER	
Algorithm parameter qualifier	'12' modulus
Algorithm parameter value	CA3's public key
ALGORITHM PARAMETER	
Algorithm parameter qualifier	'14' modulus length
Algorithm parameter value	'1024'

SECURITY RESULT	**Digital signature of the certificate by CA3**
VALIDATION RESULT	
Validation value qualifier	'1' unique validation value
Validation value	the filtered 1024 Bit digital signature

E.4 Symmetric key delivery

E.4.1 Narrative

An organization O2 delivers a symmetric key to organization O1, encrypted under a previously agreed key encrypting key KEK1, following an earlier symmetric key request from the organization O1 to organization O2. The request message could be referred to explicitly by using the USX segment between the USE and USF segments.

E.4.2 Security details

SECURITY MESSAGE RELATION	
MESSAGE RELATION	'2' response

KEY MANAGEMENT FUNCTION	
KEY MANAGEMENT FUNCTION QUALIFIER	'251' symmetric key delivery
FILTER FUNCTION	'2' hexadecimal filter

SECURITY ALGORITHM	
SECURITY ALGORITHM	
Use of algorithm	'5' owner enciphering
Cryptographic mode of operation	'2' CBC
Algorithm	'1' DES
ALGORITHM PARAMETER	
Algorithm parameter qualifier	'5' symmetric key encrypted under a symmetric key
Algorithm parameter value	the filtered encrypted key value: '3A94BACCF7DE11A5BEAD5320A2F493'
ALGORITHM PARAMETER	
Algorithm parameter qualifier	'10' key encrypting key name
Algorithm parameter value	'KEK1'

ICS 35.240.60

Price based on 22 pages