UNITED
NATIONS

E

Economic and Social
Council

Distr.
RESTRICTED

TRADE/WP.4/R.1249
31 January 1997

ENGLISH ONLY

ECONOMIC COMMISSION FOR EUROPE

COMMITTEE ON THE DEVELOPMENT OF TRADE

Working Party on Facilitation of
International Trade Procedures
(Item 3 of the provisional agenda of
the Meetings of Experts on Data Elements
and Automatic Data Interchange (GE.1)
Fifty-fifth session, 19-20 March 1997)

ELECTRONIC DATA INTERCHANGE FOR ADMINISTRATION, COMMERCE AND TRANSPORT (EDIFACT) - APPLICATION LEVEL SYNTAX RULES

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

* * *

Submitted by the Syntax Development Group *

As requested during the September 1996 sessions of GE.1 and WP.4, this document presents part 9 of the final draft of the revised EDIFACT syntax as prepared by the Syntax Development Group and will upon approval be submitted to ISO. It takes into account comments received on the previous version.
The Group of Experts is invited to:
approve this document.

* The present document is reproduced in the form in which it was received by the secretariat.

ISO 9735-9

Release 2
1997-01-24

Electronic data interchange for administration, commerce and transport (EDIFACT) - Application level syntax rules

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

Contents

	Page
Foreword	4
Introduction	5
1 Scope	**6**
2 Conformance	**6**
3 References	**6**
4 Definitions	**6**
5 Rules for the use of the security key and certificate management message	**7**
Annex A: Definitions	**11**
Annex B: Syntax service directories (segments, composite data elements and simple data elements)	**12**
Annex C: KEYMAN functions	**20**
Annex D: Security techniques to be applied to KEYMAN messages	**25**
Annex E: Use of segment groups in KEYMAN messages	**26**
Annex F: A model for key management	**28**
Annex G: Syntax service code directory	**30**
Annex H: Key and certificate management examples	**32**

Foreword

(To be amended as necessary, according to ISO procedures)

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.

Draft International Standards adopted by the technical committees are circulated to the member bodies for approval before their acceptance as International Standards by the ISO Council. They are approved in accordance with ISO procedures requiring at least 75% approval by the member bodies voting.

International Standard ISO 9735 Release 3 was prepared by the UN/ECE Trade Division (as UN/EDIFACT) and was adopted, under the "fast-track procedure" as an existing standard, by Technical Committee ISO TC 154, *Documents and data elements in administration; commerce and industry.*

ISO 9735 consists (currently) of the following parts, under the general Title *Electronic Data Interchange For Administration, Commerce And Transport (EDIFACT) - Application level syntax rules:*

ISO 9735-1	-	*Syntax rules common to all parts together with the syntax service directories*
ISO 9735-2	-	*Syntax rules specific to batch EDI*
ISO 9735-3	-	*Syntax rules specific to interactive EDI*
ISO 9735-4	-	*Syntax and service report message for batch EDI (message type - CONTRL)*
ISO 9735-5	-	*Security rules for batch EDI (authenticity, integrity and non-repudiation of origin)*
ISO 9735-6	-	*Secure authentication and acknowledgement message (message type - AUTACK)*
ISO 9735-7	-	*Security rules for batch EDI (confidentiality)*
ISO 9735-8	-	*Associated data in EDI*
ISO 9735-9	-	*Security key and certificate management message (message type - KEYMAN)*
ISO 9735-10	-	*Security rules for interactive EDI*

Further parts may be added in the future.
In this Part 9, annexes A and B form an integral part of this International Standard.

Introduction

This International Standard 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.

These syntax rules may be used in any application, but messages using these rules may only be referred to as EDIFACT messages if they comply with other guidelines, rules and directories in UNTDID. For UN/EDIFACT, messages shall comply with the message design rules for batch or interactive usage as applicable.

Communications specifications and protocols are outside the scope of this standard.

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

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

1 Scope

This International Standard for batch EDIFACT security defines the security key and certificate management message KEYMAN.

2 Conformance

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 are interchanged are in conformance if the structure and representation of the data conform to the syntax rules specified in this International Standard.

Devices supporting this International Standard 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 Part 1, Part 2, and Part 5 of the International Standard.

When identified in this International Standard, provisions defined in related standards shall form part of the conformance criteria.

3 Normative references

This normative text does not reference other standards.

4 Definitions

For the purpose of this International Standard, the definitions in Part 1 annex A, Part 5 annex A and annex A of this part apply.

5 Rules for the use of security key and certificate management

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 Part 5 of this international standard.

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.

Note: 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 Part 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 Part 5). This group shall be used in the request or delivery of keys and certificates.

Where it is desired to refer to a non-EDIFACT certificate (such as X.509), the certificate reference in USC (0536) shall contain the reference identification number (0802) from the UNO segment of the package containing the non-EDIFACT certificate, and no other data elements (in order to distinguish it from an EDIFACT certificate reference).

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 Part 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 Part 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 Part 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 - ie 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 (eg valid, revoked) or public keys (eg 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 Part 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 Part 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 Part 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 Part 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

5.4.3.1 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     Certifica te                      M   1         |   |
0160    USA     Security algorithm                C   3         |   |
0170    USR     Security result                   C   1     --------+

0180    UNT     Message trailer                   M   1
```

Annex A
(normative)

Definitions

Addendum - to be added to Part 1 annex A when approved

For the purpose of this International Standard, the following definitions apply:

A.1 **certification path**: An ordered sequence of certificates of objects in the Directory Information Tree which, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path. (ISO 9594-8) [1]

Annex B
(normative)
Addendum - to be added to Part 1 annex C when approved

Syntax service directories
(segments, composite data elements and simple data elements)

B.1 Segment directory

B.1.1 Legend

Function The function of the segment

POS The sequential position number of the segment or stand-alone data element or composite data element in the segment table

TAG The tags of all service segments contained in the segment directory start with the letter “U”. The tags of all service composite data elements start with the letter "S", and the tags of all service simple data elements start with the figure "0"

Name Name of a SEGMENT in capital letters
Name of a COMPOSITE DATA ELEMENT in capital letters
Name of a STAND-ALONE DATA ELEMENT in capital letters
Name of a component data element in small letters

S The status of the segment in the structure or of the stand-alone data element or composite data element in the segment, or of the components in the composite (where M = Mandatory, C = Conditional)

R The maximum number of occurrences of the segment in the structure or of the stand-alone data element or composite data element in the segment

Repr. Data value representation of the stand-alone data element or component data element in the composite.

a alphabetic characters
n numeric characters
an alphanumeric characters
a3 3 alphabetic characters, fixed length
n3 3 numeric characters, fixed length
an3 3 alphanumeric characters, fixed length
a..3 up to 3 alphabetic characters
n..3 up to 3 numeric characters
an..3up to 3 alphanumeric characters

B.1.2 Dependency note identifiers

Code	Name
D1	One and only one
D2	All or none
D3	One or more
D4	One or none
D5	If first, then all
D6	If first, then at least one more
D7	If first, then none of the others

See clause 11.5 in Part 1 for the definition of the dependency note identifiers.

B.1.3 Index of segments by tag

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

B.1.4 Index of segments by name

TAG	Name
USC	Certificate
USF	Key management function
UNH	Message header
UNT	Message trailer
USA	Security algorithm
USE	Security message relation
USX	Security references
USR	Security result
USL	Security list status

B.1.5 Segment specifications

Notes:
1. Only segments which are not included in other parts of this international standard are defined here.

USE SECURITY MESSAGE RELATION

Function: To specify the relation to earlier security messages, such as response to a particular request, or request for a particular answer.

Pos	TAG	Name	S	R	Repr.	Notes
010	0565	MESSAGE RELATION, CODED	M	1	an..3	

USF KEY MANAGEMENT FUNCTION

Function: To specify the type of key management function and the status of a corresponding key or certificate

Pos	TAG	Name	S	R	Repr.	Notes
010	0579	KEY MANAGEMENT FUNCTION QUALIFIER	M	1	an..3	
020	S504	LIST PARAMETER	C	9		
	0575	List parameter qualifier	M		an..3	
	0558	List parameter	M		an..70	
030	0567	SECURITY STATUS, CODED	C	1	an..3	
040	0572	CERTIFICATE SEQUENCE NUMBER	C	1	n..4	
050	0505	FILTER FUNCTION, CODED	C	1	an..3	

USL SECURITY LIST STATUS

Function: To specify the status of security objects, such as keys or certificates to be delivered in a list, and the corresponding list parameters.

Pos	TAG	Name	S	R	Repr.	Notes
010	0567	SECURITY STATUS, CODED	M	1	an..3	
020	S504	LIST PARAMETER	C	9		
	0575	List parameter qualifier	M		an..3	
	0558	List parameter	M		an..70	

B.2 Composite data element directory

B.2.1 Legend

POS The sequential position number of the component data element in the composite data element

TAG The tags of all service composite data elements contained in the composite data element directory start with the letter "S", and all service simple data elements start with the figure "0"

Name Name of a component data element in small letters

S The status of the component data element in the composite data element (where M = Mandatory and C = Conditional)

Repr. Data value representation of the component data element in the composite.

a	alphabetic characters
n	numeric characters
an	alphanumeric characters
a3	3 alphabetic characters, fixed length
n3	3 numeric characters, fixed length
an3	3 alphanumeric characters, fixed length
a..3	up to 3 alphabetic characters
n..3	up to 3 numeric characters
an..3	up to 3 alphanumeric characters

Desc. Description of the composite data element

B.2.2 Dependency note identifiers

Code	Name
D1	One and only one
D2	All or none
D3	One or more
D4	One or none
D5	If first, then all
D6	If first, then at least one more
D7	If first, then none of the others

See clause 11.5 in Part 1 for the definition of the dependency note identifiers.

B.2.3 Index of composite data elements by tag

Notes:
1. Only composite data elements which are not included in other parts of this international standard are included here.

TAG	Name
S504	List parameter

B.2.4 Index of composite data elements by name

TAG	Name
S504	List parameter

B.2.5 Composite data element specifications

S504 LIST PARAMETER

Desc : Identification of a parameter for a list request or delivery

POS	TAG	Name	S	Repr.	Notes
010	0575	List parameter qualifier	M	an..3	
020	0558	List parameter	M	an..70	

B.3 Simple data element directory

B.3.1 Legend

The tags of all service simple data elements contained in the simple data element directory start with the figure “0”.

Name Name of a simple data element

Desc. Description of the simple data element

Repr. Data value representation of the simple data element :

a	alphabetic characters
n	numeric characters
an	alphanumeric characters
a3	3 alphabetic characters, fixed length
n3	3 numeric characters, fixed length
an3	3 alphanumeric characters, fixed length
a..3	up to 3 alphabetic characters
n..3	up to 3 numeric characters
an..3	up to 3 alphanumeric characters

Notes Simple data element note number(s)

B.3.2 Index of simple data elements by tag

Notes:
1. Only data elements which are not included in other parts of this international standard are defined here.

TAG	Name
0558	List parameter
0565	Message relation, coded
0572	Certificate sequence number
0575	List parameter qualifier
0579	Key management function qualifier

B.3.3 Index of simple data elements by name

TAG	Name
0572	Certificate sequence number
0579	Key management function qualifier
0558	List parameter
0575	List parameter qualifier
0565	Message relation, coded

B.3.4 Simple data element specifications

0558 LIST PARAMETER

Desc : Specification of the list requested or delivered.

Repr : an..70

0565 MESSAGE RELATION, CODED

Desc : Relationship with another message, past or future

Repr : an..3

0572 CERTIFICATE SEQUENCE NUMBER

Desc : Specification of a certificate’s position within a certification path

Repr : n..4

Note 1: Allows certification paths to be ordered by specifying the ordinal number of the certificate within a certification path.

0575 LIST PARAMETER QUALIFIER

Desc : Specification of the type of list parameter.

Repr : an..3

0579 KEY MANAGEMENT FUNCTION QUALIFIER

Desc : Specification of the type of key management function

Repr : an..3

Annex C
(informative)

KEYMAN functions

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, ie 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.

C.1 Registration-related key management functions

C.1.1 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 Part 5 of this international standard may be useful, if further secured out of band.

C.1.2 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.

C.2 Certification-related key management functions

C.2.1 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 Part 5 of this international standard 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.

C.2.2 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 Part 5, by the private key certified by the certificate to be renewed.

C.2.3 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 Part 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.

C.2.4 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.

C.2.5 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.

C.2.6 Certificate status request

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

C.2.7 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.

C.2.8 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.

C.2.9 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.

C.3 Revocation-related key management functions

C.3.1 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.

C.3.2 Revocation confirmation

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

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

C.3.3 Revocation list request

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

C.3.4 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.

C.4 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.

C.5 Certificate paths

C.5.1 Certificate path delivery

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

C.6 Symmetric key generation and transport

C.6.1 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.

C.6.2 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.

C.7 Key discontinuation

C.7.1 (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.

C.7.2 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 D
(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 Part 5 of this international standard, to be used with each KEYMAN function.

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 E
(informative)

Use of segment groups in KEYMAN messages

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

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

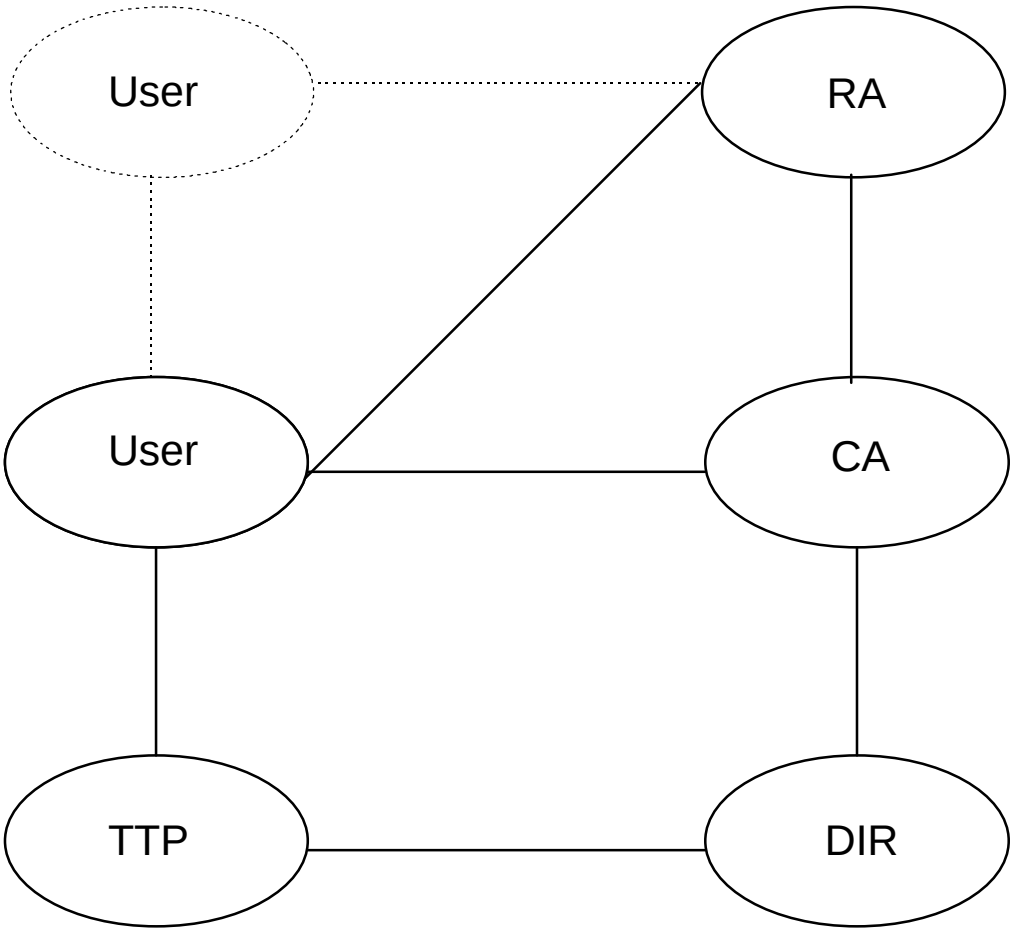
Deliveries or notices

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

Annex F
(informative)

A model for key management

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 the following figure, where five logical parties are defined according to their functionality:



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 characterised 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.

F.1 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.

F.2 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.

F.3 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. In stead, 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.

F.4 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.

F.5 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 G
(informative)
Addendum - to be added to Part 1 annex D when approved

Syntax service code directory

The tags of all simple data elements contained in the simple data element directory start with the figure “0”.

```
-----------------------------------------------------------------------

  0565  Message relation, coded

  Desc: Relationship with another message, past or future.

  Repr: an..3

        1 No relation
             The message is initial.
        2 Response
             The message is a response message.
        3 Response requested
             The message requests an answer.

-----------------------------------------------------------------------

  0575  List parameter qualifier

  Desc: Specification of the type of list parameter.

  Repr: an..3

      ZZZ Mutually defined
             Self explanatory.

-----------------------------------------------------------------------


  0579  Key management function qualifier

  Desc: Specification of the type of key management function.

  Repr: an..3

      101 Registration submission
             Submission of information for registration.
      102 Asymmetric key pair request
             Request a trusted party to generate an asymmetric key pair.
      110 Certification request
             Request certification of credentials and public key.
      111 Certificate renewal request
             Request to extend the validity period of the current valid
             key, whose certificate is about to expire.
      112 Certificate replacement request
             Request to replace the current certificate by a new one with
             a different public key (and possibly other information).
      121 Certificate (path) retrieval request
             Request the delivery of an existing (valid or revoked)
             certificate, with path details where appropriate.
      123 Certificate list retrieval request
```

Request full or partial list of certificates.

124 Certificate status request
Request current status of a given certificate.

125 Certificate validation request
Request the CA to validate an existing certificate.

126 Certificate delivery request
Request the CA to deliver a (valid or revoked) certificate to a list of recipients known to the CA or specified elsewhere.

130 Revocation request
Request revocation of a party's certificate.

131 Alert request
Request to put a party's certificate on alert.

140 Revocation list request
Request full or partial list of revoked certificates.

150 Symmetric key request
Request the delivery of symmetric keys.

151 Symmetric key discontinuation request
Request discontinuation of symmetric key.

152 Asymmetric key discontinuation request
Request discontinuation of asymmetric key.

221 Certificate delivery
Delivery of an existing (valid or revoked) certificate.

222 Certificate path delivery
Delivery of a path.

224 Certificate status notice
Notice of current status of a given certificate.

225 Certificate validation notice
Notice of validation of an existing certificate.

231 Revocation Confirmation
Confirmation of revocation of a party's certificate.

241 Revocation list delivery
Delivery of full or partial list of revoked certificates.

251 Symmetric key delivery
Delivery of symmetric keys.

252 Discontinuation acknowledgement
Acknowledgement of the requested discontinuation.

Annex H
(informative)

Key and certificate management examples

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

H.1 Revocation request

H.1.1 Narrative

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

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

H.2 Symmetric key discontinuation request

H.2.1 Narrative

Organisation O1 requests organisation O2 to stop using a mutual symmetric key K1 because it has been superseded. This message between the organisations will be protected for message origin authentication by the organisation in the normal way using security header and trailer segment groups as described in Part 5 of this international standard using another previously agreed symmetric key. The message may be responded to by a discontinuation acknowledgement from O2 to O1.

H.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 Cryptographic mode of operation Algorithm	 ‘2’ owner symmetric ‘2’ CBC ‘1’ DES
ALGORITHM PARAMETER Algorithm parameter qualifier Algorithm parameter value	 ‘9’ symmetric key name ‘K1’

H.3 Certificate (path) delivery

H.3.1 Narrative

This message from certification authority CA2 to an organisation O1 follows an earlier certificate (path) retrieval request from the organisation to their certification authority for the path of organisation 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 2 years. The CA1, CA3 and O2 public key lengths are 2048, 1024 and 512 respectively. All public key exponents are 10001_{16}.

H.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 Key name Security party identification Security party code list qualifier Security party code list responsible agency	 ‘3’ certificate owner ‘CA3’ O2’s certification authority ‘ZZZ’ mutually agreed ‘1’ UN
SECURITY IDENTIFICATION DETAILS Security party qualifier Key name Security party identification Security party code list qualifier Security party code list responsible agency	 ‘4’ authenticating party ‘CA1’ the top level certification authority ‘ZZZ’ mutually agreed ‘1’ UN
CERTIFICATE SYNTAX 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 Service character for signature	 ‘1’ segment terminator ‘27’ apostrophe
SERVICE CHARACTER FOR SIGNATURE Service character for signature qualifier Service character for signature	 ‘2’ composite data element separator ‘2B’ plus sign
SERVICE CHARACTER FOR SIGNATURE Service character for signature qualifier Service character for signature	 ‘3’ data element separator ‘3A’ colon
SERVICE CHARACTER FOR SIGNATURE Service character for signature qualifier Service character for signature	 ‘4’ release character ‘3F’ question mark
SERVICE CHARACTER FOR SIGNATURE Service character for signature qualifier Service character for signature	 ‘5’ repetition separator ‘2A’ asterisk
SECURITY DATE AND TIME Date and time qualifier Event date Event time Time offset	 ‘2’ certificate generation date and time ‘19961201’ ‘000000’ ‘0000’
SECURITY DATE AND TIME Date and time qualifier Event date Event time Time offset	 ‘3’ certificate start of validity period ‘19970101’ ‘000000’ ‘0000’
SECURITY DATE AND TIME Date and time qualifier Event date Event time Time offset	 ‘4’ certificate end of validity period ‘20070101’ ‘000000’ ‘0000’
SECURITY STATUS	‘1’ valid

SECURITY ALGORITHM	
SECURITY ALGORITHM Use of algorithm Cryptographic mode of operation Algorithm	 ‘6’ owner signing ‘10’ RSA
ALGORITHM PARAMETER Algorithm parameter qualifier Algorithm parameter value	 ‘13’ exponent ‘010001’
ALGORITHM PARAMETER Algorithm parameter qualifier Algorithm parameter value	 ‘12’ modulus CA3’s public key
ALGORITHM PARAMETER Algorithm parameter qualifier Algorithm parameter value	 ’14’ modulus length ‘1024’

SECURITY ALGORITHM	
SECURITY ALGORITHM Use of algorithm Cryptographic mode of operation Algorithm	 ‘4’ issuer hashing ‘11’ HDS2 ‘1’ DES

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

SECURITY RESULT	Digital signature of the certificate by CA1
VALIDATION RESULT Validation value qualifier Validation value	 Digital signature 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 Key name Security party identification Security party code list qualifier Security party code list responsible agency	 ‘3’ certificate owner ‘O2’ organisation O2 ‘ZZZ’ mutually agreed ‘1’ UN
SECURITY IDENTIFICATION DETAILS Security party qualifier Key name Security party identification Security party code list qualifier Security party code list responsible agency	 ‘4’ authenticating party ‘CA3’ O2’s certification authority ‘ZZZ’ mutually agreed ‘1’ UN
CERTIFICATE SYNTAX 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 Service character for signature	 ‘1’ segment terminator ‘27’ apostrophe
SERVICE CHARACTER FOR SIGNATURE Service character for signature qualifier Service character for signature	 ‘2’ composite data element separator ‘2B’ plus sign
SERVICE CHARACTER FOR SIGNATURE Service character for signature qualifier Service character for signature	 ‘3’ data element separator ‘3A’ colon
SERVICE CHARACTER FOR SIGNATURE Service character for signature qualifier Service character for signature	 ‘4’ release character ‘3F’ question mark
SERVICE CHARACTER FOR SIGNATURE Service character for signature qualifier Service character for signature	 ‘5’ repetition separator ‘2A’ asterisk
SECURITY DATE AND TIME Date and time qualifier Event date Event time Time offset	 ‘2’ certificate generation date and time ‘19970201’ ‘000000’ ‘0000’
SECURITY DATE AND TIME Date and time qualifier Event date Event time Time offset	 ‘3’ certificate start of validity period ‘19970301’ ‘000000’ ‘0000’
SECURITY DATE AND TIME Date and time qualifier Event date Event time Time offset	 ‘4’ certificate end of validity period ‘19990301’ ‘000000’ ‘0000’
SECURITY STATUS	‘1’ valid

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

SECURITY ALGORITHM	
SECURITY ALGORITHM Use of algorithm Cryptographic mode of operation Algorithm	 ‘4’ issuer hashing ‘11’ HDS2 ‘1’ DES

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

SECURITY RESULT	Digital signature of the certificate by CA3
VALIDATION RESULT Validation value qualifier Validation value	 Digital signature the filtered 1024 Bit digital signature

H.4 Symmetric key delivery

H.4.1 Narrative

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

H.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 Cryptographic mode of operation Algorithm	 ‘5’ owner enciphering ‘2’ CBC ‘1’ DES
ALGORITHM PARAMETER Algorithm parameter qualifier Algorithm parameter value	 ‘5’ symmetric key encrypted under a symmetric key the filtered encrypted key
ALGORITHM PARAMETER Algorithm parameter qualifier Algorithm parameter value	 ‘10’ key encrypting key name ‘KEK1’