INTERNATIONAL STANDARDIZED PROFILE

ISO/IEC ISP 10611-3

Third edition
2003-06-15

Information technology — International Standardized Profiles AMH1n — Message Handling Systems — Common Messaging —

Part 3: AMH11 — Message Transfer (P1)

Technologies de l'information — Profils normalisés internationaux AMH1n — Systèmes de messagerie — Messagerie commune —

Partie 3: AMH11 — Transfert de messages (P1)

Reference number
ISO/IEC ISP 10611-3:2003(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.org
Web www.iso.org

Published in Switzerland

Contents

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

In addition to developing International Standards, ISO/IEC JTC 1 also develops International Standardized Profiles. An International Standardized Profile is an internationally agreed, harmonized document which identifies a standard or group of standards, together with options and parameters, necessary to accomplish a function or a set of functions. Draft International Standardized Profiles adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standardized Profile requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC ISP 10611-3 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 6, *Telecommunications and information exchange between systems*.

This third edition cancels and replaces the second edition (ISO/IEC ISP 10611-3:1997), which has been technically revised.

ISO/IEC ISP 10611 consists of the following parts, under the general title *Information technology — International Standardized Profiles AMH1n — Message Handling Systems — Common Messaging*:

— *Part 1: MHS Service Support*

— *Part 2: Specification of ROSE, RTSE, ACSE, Presentation and Session Protocols for use by MHS*

— *Part 3: AMH11 — Message Transfer (P1)*

— *Part 4: AMH12 and AMH14 — MTS Access (P3) and MTS 94 Access (P3)*

— *Part 5: AMH13 — MS Access (P7)*

— *Part 6: AMH15 — MS 94 Access (P7)*

Introduction

This part of ISO/IEC ISP 10611 is defined within the context of Functional Standardization, in accordance with the principles specified by ISO/IEC TR 10000, “Framework and Taxonomy of International Standardized Profiles”. The context of Functional Standardization is one part of the overall field of Information Technology (IT) standardization activities, covering base standards, profiles, and registration mechanisms. A profile defines a combination of base standards that collectively perform a specific well-defined IT function. Profiles standardize the use of options and other variations in the base standards, and provide a basis for the development of uniform, internationally recognized system tests.

One of the rôles for an ISP is to serve as the basis for the development (by organizations other than ISO and IEC) of internationally recognized tests. ISPs are produced not simply to legitimize' a particular choice of base standards and options, but to promote real system interoperability. The development and widespread acceptance of tests based on this and other ISPs is crucial to the successful realization of this goal.

The text for this part of ISO/IEC ISP 10611 was originally developed in close cooperation between the MHS Expert Groups of the three Regional Workshops: the North American OSE Implementors' Workshop (OIW), the European Workshop for Open Systems (EWOS) (jointly with the corresponding expert group of the European Telecommunications Standards Institute - ETSI) and the OSI Asia-Oceania Workshop (AOW). The first and second editions of this part of ISO/IEC ISP 10611 were harmonized between these three Workshops and ratified by the plenary assemblies of all three Workshops.

Responsibility for maintenance and further development of MHS ISPs has been transferred to ISO/IEC JTC1/SC33/WG1, who have produced this edition to encompass additions and corrections to ISO/IEC 10021. Because new core requirements have been added for support of Universal Characters in addresses which will take time to be implemented within MHS systems, it is expected that the second edition of this part of ISO/IEC ISP 10611 will remain available for an overlap period.

Information technology — International Standardized Profiles AMH1n — Message Handling Systems — Common Messaging —

Part 3:
AMH11 — Message Transfer (P1)

1 Scope

1.1 General

This part of ISO/IEC ISP 10611 (AMH11) covers message transfer between message transfer agents (MTAs) using the P1 Message Transfer Protocol (see also figure 1). These specifications form part of the Common Messaging application functions, as defined in the parts of ISO/IEC ISP 10611 which form a common basis for content type-dependent International Standardized Profiles for MHS that will be developed.

An MTA which conforms to profiles AMH11n as specified in this part of ISO/IEC ISP 10611 shall support a 'normal mode' OSI protocol infrastructure (AMH111) as required by both ISO/IEC 10021-6 and the ITU-T X.400 Recommendations, and may additionally support an 'X.410 mode' OSI protocol infrastructure (AMH112) as required, for ADMDs, by the ITU-T X.400 Recommendations.

1.2 Position within the taxonomy

This part of ISO/IEC ISP 10611 is the third part of a multipart ISP identified in ISO/IEC TR 10000-2 as "AMH1, Message Handling Systems - Common Messaging".

This part of ISO/IEC ISP 10611 specifies the following profiles:

AMH111 - Message Transfer (P1) - Normal mode

AMH112 - Message Transfer (P1) - X.410(1984) mode

The AMH11n profiles may be combined with any T-Profiles (see ISO/IEC TR 10000) specifying the OSI connection-mode Transport service.

1.3 Scenario

The model used is one of two or more MTAs intercommunicating within a Message Transfer System (MTS) using the P1 protocol, as shown in figure 1.

Figure 1 - AMH11n scenario

NOTE - In an ITU-T context, a domain may be treated as an MTA for the purposes of conformance to the AMH11n profiles.

The AMH11n profiles cover all aspects of the MTA Abstract Service, as defined in clause 12 of ISO/IEC 10021-4, when realized using the P1 protocol.

The OSI upper layer services and protocols to support the Message Handling Systems functions covered by the AMH11n profiles are specified in the set of standards identified in table 1.

Table 1 - AMH11n profile model

Application Layer	MHS	ISO/IEC 10021-6
	RTSE	see ISO/IEC ISP 10611-2
	ACSE	see ISO/IEC ISP 10611-2
Presentation Layer		see ISO/IEC ISP 10611-2
Session Layer		see ISO/IEC ISP 10611-2

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

Amendments and corrigenda to the base standards referenced are listed in annex B.

NOTES

1 - References in the body of this part of ISO/IEC ISP 10611 to specific clauses of ISO/IEC documents shall be considered to refer also to the corresponding clauses of the equivalent ITU-T Recommendations (as noted below) unless otherwise stated.

2 - Informative references are found in annex C.

ISO/IEC TR 10000-1:1998, *Information technology - Framework and taxonomy of International Standardized Profiles - Part 1: General principles and documentation framework*

ISO/IEC TR 10000-2:1998, *Information technology - Framework and taxonomy of International Standardized Profiles - Part 2: Principles and Taxonomy for OSI Profiles*

ITU-T Recommendation F.400/X.400 (1999), *Message Handling Systems - System and service overview*

ISO/IEC 10021-1:2003, *Information technology - Message Handling Systems (MHS) - Part 1: System and Service Overview [see also ITU-T Recommendation F.400/X.400]*

ITU-T Recommendation X.402 (1999) | ISO/IEC 10021-2: [1], *Information technology - Message Handling Systems (MHS) - Overall architecture*

ITU-T Recommendation X.411 (1999) | ISO/IEC 10021-4: [2], *Information technology - Message Handling Systems (MHS) - Message Transfer System: Abstract service definition and procedures*

ITU-T Recommendation X.419 (1999), *Message Handling Systems - Protocol Object Identifiers*

ISO/IEC ISP 10611-1:2003, *Information technology - International Standardized Profiles AMH1n - Message Handling Systems - Common Messaging - Part 1: MHS Service Support*

1) To be published. (Revision of ISO/IEC 10021-2:1996)

2) To be published. (Revision of ISO/IEC 10021-4:1997)

ISO/IEC ISP 10611-2:1997, *Information technology - International Standardized Profiles AMH1n - Message Handling Systems - Common Messaging - Part 2: Specification of ROSE, RTSE, ACSE, Presentation and Session Protocols for use by MHS*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

Terms used in this part of ISO/IEC ISP 10611 are defined in the referenced base standards; in addition, the following terms are defined.

3.1 General

Basic requirement : an Element of Service, protocol element, procedural element or other identifiable feature specified in the base standards which is required to be supported by all MHS implementations.

Functional group : a specification of one or more related Elements of Service, protocol elements, procedural elements or other identifiable features specified in the base standards which together support a significant optional area of MHS functionality.

NOTE - A functional group can cover any combination of MHS features specified in the base standards for which the effect of implementation can be determined at a standardized external interface - i.e. via a standard OSI communications protocol (other forms of exposed interface, such as a standardized programmatic interface, are outside the scope of this version of ISO/IEC ISP 10611).

3.2 Support classification

To specify the support level of arguments, results and other protocol features for this part of ISO/IEC ISP 10611, the following terminology is defined.

The following classifications are used in this part of ISO/IEC ISP 10611 to specify static conformance requirements - i.e. capability.

In the case of protocol elements, the classification is relative to that of the containing element, if any. Where the constituent elements of a non-primitive element are not individually specified, then each shall be considered to have the classification of that element. Where the range of values to be supported for an element is not specified, then all values defined in the MHS base standards shall be supported.

mandatory full support (**m**) : the element or feature shall be fully supported. An implementation shall be able to generate the element and/or receive the element and perform all associated procedures (i.e. implying the ability to handle both the syntax and the semantics of the element) as relevant, as specified in the MHS base standards. The receiving capability shall be considered to include relaying where appropriate. Where support for origination (generation) and reception are not distinguished, then both capabilities shall be assumed.

mandatory minimal support (**m-**) : the element shall be supported. However, an implementation is only required to be able to copy the syntax of the element to the corresponding element of a message, probe or report for onward transfer or delivery, as appropriate, according to the procedures as specified in the MHS base standards, unless further qualified for the output envelope in question elsewhere in this multipart ISP (i.e. the classification of the output envelope takes precedence). An implementation is not required to be able to take any explicit action based on the semantics of such an element other than to treat the element as supported for criticality purposes. An implementation is not required to be able to originate such an element.

NOTE - The m- classification is designed to distinguish those cases where the MHS base standards define more than one level of functionality and the minimum required level of support in this profile is the minimum functionality defined in the base standards. Where the only functionality defined in the base standards is copying the element as described above, then the m classification is used in preference to m-.

optional support (**o**) : an implementation is not required to support the element. If support is claimed, the element shall be treated as if it were specified as mandatory support. If support is not claimed, and the element is an argument, then an implementation shall generate an appropriate error indication if the element is received. If support is not claimed, and the element is a result, then an implementation may ignore the element if it is received.

conditional support (**c**) : the element shall be supported under the conditions specified in this part of ISO/IEC ISP 10611. If these conditions are met, the element shall be treated as if it were specified as mandatory support. If these conditions are not met, the element shall be treated as if it were specified as optional support (unless otherwise stated).

out of scope (**i**) : the element is outside the scope of this part of ISO/IEC ISP 10611 - i.e. it will not be the subject of an ISP conformance test.

not applicable (**–**) : the element is not applicable in the particular context in which this classification is used.

4 Abbreviations

84IW	84 Interworking
AMH	Application Message Handling
ASN.1	Abstract Syntax Notation One
CV	Conversion
DIR	Use of Directory
DL	Distribution List
EoS	Element of Service
FG	Functional group
ISP	International Standardized Profile
LD	Latest Delivery
MHS	Message Handling Systems
MS	Message store
MTA	Message transfer agent
OSI	Open Systems Interconnection
PD	Physical Delivery
PDAU	Physical delivery access unit
RED	Redirection
RoC	Return of Content
SEC	Security
UA	User agent

Support level for protocol elements and features (see 3.2):

m	mandatory full support
m-	mandatory minimal support
o	optional support
c	conditional support
i	out of scope
–	not applicable
r	required
x	excluded

5 Conformance

This part of ISO/IEC ISP 10611 states requirements upon implementations to achieve interworking. A claim of conformance to this part of ISO/IEC ISP 10611 is a claim that all requirements in the relevant base standards are satisfied, and that all requirements in the following clauses and in annex A of this part of ISO/IEC ISP 10611 are satisfied. Annex A states the relationship between these requirements and those of the base standards.

5.1 Conformance statement

For each implementation claiming conformance to profiles AMH11n as specified in this part of ISO/IEC ISP 10611, a PICS shall be made available stating support or non-support of each option identified in this part of ISO/IEC ISP 10611.

The scope of conformance to profiles AMH11n is restricted to MTAs that support message transfer. A claim of conformance to profiles AMH11n shall confirm that the implementation supports profile AMH111 and shall state whether the implementation also supports profile AMH112 (jointly referenced as AMH11 in this part of ISO/IEC ISP 10611 where a distinction is unnecessary).

5.2 MHS conformance

This part of ISO/IEC ISP 10611 specifies implementation options or selections such that conformant implementations will satisfy the conformance requirements of ISO/IEC 10021 and optionally those of the ITU-T X.400 Recommendations.

Implementations conforming to profile AMH11 as specified in this part of ISO/IEC ISP 10611 shall implement all the mandatory support (m or m-) features identified as basic requirements in annex A except those features that are components of an unimplemented optional feature. It shall be stated which optional support (o) features are implemented.

For implementations conforming to profile AMH11 as specified in this part of ISO/IEC ISP 10611, it shall be stated whether or not they support any of the optional functional groups as specified in ISO/IEC ISP 10611-1 which are applicable to the scope of this profile. Implementations conforming to profile AMH112 shall support the 84 Interworking functional group. For each functional group for which support is claimed, an implementation shall implement all the mandatory support (m or m-) features identified for that functional group in annex A except those features that are components of an unimplemented optional feature. It shall be stated which optional support (o) features are implemented.

Implementations shall support the procedures associated with supported protocol elements as specified in the base standards and as further specified in ISO/IEC ISP 10611-1. The MHS Elements of Service corresponding to such procedures are indicated in annex A of ISO/IEC ISP 10611-1.

For implementations conforming to profile AMH11 as specified in this part of ISO/IEC ISP 10611, the P1 application context(s) for which conformance is claimed shall be stated. Implementations conforming to profile AMH111 shall support the P1 mts-transfer application context. Implementations conforming to profile AMH112 shall also support the P1 mts-transfer-protocol and mts-transfer-protocol-1984 application contexts. Implementations conforming to profile AMH111 which also support the P1 mts-transfer-protocol-1984 application context shall support the 84 Interworking functional group.

5.3 Underlying layers conformance

Implementations conforming to profile AMH11 as specified in this part of ISO/IEC ISP 10611 shall also conform to ISO/IEC ISP 10611-2 in accordance with the P1 application context(s) for which conformance is claimed.

(Blank page)

Annex A[3]

(normative)

ISPICS Proforma

for ISO/IEC ISP 10611-3 (AMH11)

In the event of a discrepancy becoming apparent in the body of this part of ISO/IEC ISP 10611 and the tables in this annex, this annex is to take precedence.

Clause A.1 specifies the basic requirements for conformance to profile AMH11. Clause A.2 specifies additional requirements to those specified in A.1 for each of the optional functional groups if conformance to such a functional group is claimed. Clause A.3 allows additional information to be provided for certain aspects of an implementation where no specific requirements are included in ISO/IEC ISP 10611. All three clauses shall be completed as appropriate.

In each table, the "Base" column reflects the level of support required for conformance to the base standard and the "Profile" column specifies the level of support required by this ISP (using the classification and notation defined in 3.2).

The “Ref” column is provided for cross-referencing purposes. The notation employed for references also indicates composite elements which contain sub-elements (a sub-element reference is prefixed by the reference of the composite element).

The “Support” column is provided for completion by the supplier of the implementation as follows:

Y	the element or feature is fully supported (i.e. satisfying the requirements of the m profile support classification)
Y-	the element or feature is minimally supported (i.e. satisfying the requirements of the m-profile support classification)
N	the element or feature is not supported, further qualified to indicate the action taken on receipt of such an element as follows: ND - the element is discarded/ignored NR - the PDU is rejected (with an appropriate error indication where applicable)
– or blank	the element or feature is not applicable (i.e. a major feature or composite protocol element which includes this element or feature is not supported or is minimally supported)

[3] **Copyright release for ISPICS proformas**
Users of this International Standardized Profile may freely reproduce the ISPICS proforma in this annex so that it can be used for its intended purpose and may further publish the completed ISPICS.

A.0 Identification of the implementation

A.0.1 Identification of PICS

Ref	Question	Response
1	Date of statement (YYYY-MM-DD)	
2	PICS serial number	
3	System conformance statement cross reference	

A.0.2 Identification of IUT

Ref	Question	Response
1	Implementation name	
2	Implementation version	
3	Hardware name	
4	Hardware version	
5	Operating system name	
6	Operating system version	
7	Special configuration	
8	Other information	

A.0.3 Identification of supplier

Ref	Question	Response
1	Organization name	
2	Contact name(s)	
3	Address	
4	Telephone number	
5	Telex number	
6	Fax number	
7	E-mail address	
8	Other information	

A.0.4 Identification of protocol

Ref	Question	Response
1	Title, reference number and date of publication of the protocol standard	
2	Protocol version(s)	not applicable
3	Addenda/amendments/corrigenda implemented	
4	Defect reports implemented	not applicable
NOTE - There is no change in the protocol version, as defined in the protocol, between the base standards published in 1988, 1990, 1992, 1996 and 1999.		

A.0.5 Global statement of conformance

Ref	Question	Response	Comments
1	Are all mandatory base standards requirements implemented?		

A.0.6 Statement of profile conformance

Ref	Question	Response	Comments
1	Are all mandatory requirements of profile AMH111 implemented?		
2	Are all mandatory requirements of profile AMH112 implemented?		
3	Are all mandatory requirements of any of the following optional functional groups implemented?		
3.1	Conversion (CV)		
3.2	Distribution List (DL)		class(es):
3.3	Physical Delivery (PD)		
3.4	Redirection (RED)		
3.5	Latest Delivery (LD)		
3.6	Return of Contents (RoC)		
3.7	Security (SEC)		class(es):
3.8	Use of Directory (DIR)		class(es):
3.9	84 Interworking (84IW)		

A.1 Basic requirements

A.1.1 Initiator/responder capability

Ref	Capability	Base	Profile	Support
1	Initiator	m	m	
2	Responder	m	m	

A.1.2 Supported application contexts

Ref	Application Context	Base	Profile	Support	Notes/References
1	mts-transfer	m	m		
2	mts-transfer-protocol	o	c[1]		
3	mts-transfer-protocol-1984	c[3]	c[2]		

1 if conformance to AMH112 is claimed then m else o

2 if conformance to AMH112 or the 84 Interworking functional group is claimed then m else o

3 Mandatory for MTAs operating as ADMD else optional

A.1.3 Supported operations

A.1.3.1 Bind and Unbind

Ref	Operation	Base	Profile	Support	Notes/References
1	MTABind	m	m		see A.1.4.1
2	MTAUnbind	m	m		

A.1.3.2 Message Transfer Service Element (MTSE)

Ref	Operation	Base	Profile	Support	Notes/References
1	MessageTransfer	m	m		see A.1.4.2
2	ReportTransfer	m	m		see A.1.4.3
3	ProbeTransfer	m	m		see A.1.4.4

A.1.4 Operation arguments/results

A.1.4.1 MTABind

Ref	Element	Base	Profile	Support	Notes/References
1	ARGUMENT				
1.1	NULL	m	m		
1.2	SET	m	m		
1.2.1	initiator-name	m	m		
1.2.2	initiator-credentials	m	m		
1.2.2.1	simple	m	m		
1.2.2.1.1	octet-string	o	m		
1.2.2.1.2	ia5-string	o	c[1]		
1.2.2.2	strong	o	o		
1.2.2.2.1	bind-token	m	m		
1.2.2.2.1.1	signature-algorithm-identifier	m	m		
1.2.2.2.1.2	name	m	m		
1.2.2.2.1.3	time	m	m		
1.2.2.2.1.4	signed-data	o	o		
1.2.2.2.1.5	encryption-algorithm-identifier	o	o		
1.2.2.2.1.6	encrypted-data	o	o		
1.2.2.2.2	certificate	o	o		see A.1.5/9
1.2.2.2.3	certificate-selector	o	o		see A.1.5/11
1.2.3	security-context	o	o		see A.1.6/3
2	RESULT				
2.1	NULL	m	m		
2.2	SET	m	m		
2.2.1	responder-name	m	m		
2.2.2	responder-credentials	m	m		
2.2.2.1	simple	m	m		

Ref	Element	Base	Profile	Support	Notes/References
2.2.2.1.1	octet-string	o	m		
2.2.2.1.2	ia5-string	o	c[1]		
2.2.2.2	strong	o	o		
2.2.2.2.1	bind-token	m	m		
2.2.2.2.1.1	signature-algorithm-identifier	m	m		
2.2.2.2.1.2	name	m	m		
2.2.2.2.1.3	time	m	m		
2.2.2.2.1.4	signed-data	o	o		
2.2.2.2.1.5	encryption-algorithm-identifier	o	o		
2.2.2.2.1.6	encrypted-data	o	o		
2.2.2.2.2	certificate	o	o		see A.1.5/9
2.2.2.2.3	certificate-selector	o	o		see A.1.5/11
1 if the P1 **mts-transfer-protocol-1984** AC is supported then m else o					

A.1.4.2 MessageTransfer

Ref	Element	Base	Profile	Support	Notes/References
1	MessageTransferEnvelope	m	m		
1.1	(per message transfer fields)				
1.1.1	message-identifier	m	m		see A.1.5/1
1.1.2	originator-name	m	m		see A.1.7
1.1.3	original-encoded-information-types	m	m-		see A.1.5/3
1.1.4	content-type	m	m-		see A.1.5/8
1.1.5	content-identifier	m	m		
1.1.6	priority	m	m		
1.1.7	per-message-indicators	m	m		see A.1.5/4
1.1.8	deferred-delivery-time	o	m-		
1.1.9	per-domain-bilateral-information	o	m-		see A.1.5/5
1.1.10	trace-information	m	m		see A.1.5/6

Ref	Element	Base	Profile	Support	Notes/References
1.1.11	extensions	m	m		see A.1.6/1
1.1.11.1	recipient-reassignment-prohibited	o	m		
1.1.11.2	dl-expansion-prohibited	o	m		
1.1.11.3	conversion-with-loss-prohibited	o	m		
1.1.11.4	latest-delivery-time	o	m-		
1.1.11.5	originator-return-address	o	m-		see A.1.7
1.1.11.6	originator-certificate	o	m-		see A.1.5/9
1.1.11.7	content-confidentiality-algorithm-identifier	o	m-		
1.1.11.8	message-origin-authentication-check	o	m-		see A.1.6/2
1.1.11.9	message-security-label	o	m-		see A.1.6/3
1.1.11.10	content-correlator	m	m		
1.1.11.11	dl-expansion-history	m	m-		
1.1.11.12	internal-trace-information	m	m		see A.1.6/5
1.1.11.13	certificate-selectors	o	m-		see A.1.6/9
1.1.11.14	multiple-originator-certificates	o	m-		see A.1.6/11
1.1.11.15	dl-exempted-recipients	o	m-		see A.1.7
1.1.11.16	PrivateExtensions	o	o		
1.2	per-recipient-fields	m	m		
1.2.1	recipient-name	m	m		see A.1.7
1.2.2	originally-specified-recipient-number	m	m		
1.2.3	per-recipient-indicators	m	m		
1.2.4	explicit-conversion	o	m-		
1.2.5	extensions	m	m		see A.1.6/1
1.2.5.1	originator-requested-alternate-recipient	o	m-		see A.1.7
1.2.5.2	requested-delivery-method	o	m-		
1.2.5.3	physical-forwarding-prohibited	o	m-		

Ref	Element	Base	Profile	Support	Notes/References
1.2.5.4	physical-forwarding-address-request	o	m-		
1.2.5.5	physical-delivery-modes	o	m-		
1.2.5.6	registered-mail-type	o	m-		
1.2.5.7	recipient-number-for-advice	o	m-		
1.2.5.8	physical-rendition-attributes	o	m-		
1.2.5.9	physical-delivery-report-request	o	m-		
1.2.5.10	message-token	o	m-		see A.1.6/4
1.2.5.11	content-integrity-check	o	m-		
1.2.5.12	proof-of-delivery-request	o	m-		
1.2.5.13	redirection-history	m	m-		
1.2.5.14	certificate-selectors-override	o	m-		see A.1.6/10
1.2.5.15	recipient-certificate	o	m-		see A.1.5/9
1.2.5.16	IPMPerRecipientEnvelopeExtensions	o	m-		see A.1.4.2 in ISO/IEC ISP 12062-3
1.2.5.17	PrivateExtensions	o	o		
2	content	m	m		

A.1.4.3 ReportTransfer

Ref	Element	Base	Profile	Support	Notes/References
1	ReportTransferEnvelope	m	m		
1.1	report-identifier	m	m		see A.1.5/1
1.2	report-destination-name	m	m		see A.1.7
1.3	trace-information	m	m		see A.1.5/6
1.4	extensions	m	m		see A.1.6/1
1.4.1	message-security-label	o	m-		see A.1.6/3
1.4.2	redirection-history	m	m		
1.4.3	originator-and-DL-expansion-history	m	m		
1.4.4	reporting-DL-name	o	m-		see A.1.7

Ref	Element	Base	Profile	Support	Notes/References
1.4.5	reporting-MTA-certificate	o	m-		see A.1.5/9
1.4.6	report-origin-authentication-check	o	m-		see A.1.6/8
1.4.7	internal-trace-information	m	m		see A.1.6/5
1.4.8	reporting-MTA-certificate-selector	o	m-		see A.1.5/11
1.4.9	reporting-MTA-name	o	m-		see A.1.6/12
1.4.10	PrivateExtensions	o	o		
2	ReportTransferContent	m	m		
2.1	(per report transfer fields)				
2.1.1	subject-identifier	m	m		see A.1.5/1
2.1.2	subject-intermediate-trace-information	o	m		see A.1.5/6
2.1.3	original-encoded-information-types	m	m		see A.1.5/3
2.1.4	content-type	m	m		see A.1.5/8
2.1.5	content-identifier	m	m		
2.1.6	returned-content	o	m-		
2.1.7	additional-information	o	m-		
2.1.8	extensions	m	m		see A.1.6/1
2.1.8.1	content-correlator	m	m		
2.1.8.2	PrivateExtensions	o	o		
2.2	per-recipient-fields	m	m		
2.2.1	actual-recipient-name	m	m		see A.1.7
2.2.2	originally-specified-recipient-number	m	m		
2.2.3	per-recipient-indicators	m	m		
2.2.4	last-trace-information	m	m		see A.1.5/7
2.2.5	originally-intended-recipient-name	m	m		see A.1.7
2.2.6	supplementary-information	o	m-		
2.2.7	extensions	m	m		see A.1.6/1
2.2.7.1	redirection-history	m	m		

Ref	Element	Base	Profile	Support	Notes/References
2.2.7.2	physical-forwarding-address	o	m-		see A.1.7
2.2.7.3	recipient-certificate	o	m-		see A.1.5/9
2.2.7.4	proof-of-delivery	o	m-		see A.1.6/7
2.2.7.5	recipient-certificate-selector	o	m-		see A.1.5/11
2.2.7.6	PrivateExtensions	o	o		

A.1.4.4 ProbeTransfer

Ref	Element	Base	Profile	Support	Notes/References
1	ProbeTransferEnvelope	m	m		
1.1	(per probe transfer fields)				
1.1.1	probe-identifier	m	m		see A.1.5/1
1.1.2	originator-name	m	m		see A.1.7
1.1.3	original-encoded-information-types	m	m-		see A.1.5/3
1.1.4	content-type	m	m-		see A.1.5/8
1.1.5	content-identifier	m	m		
1.1.6	content-length	m	m		
1.1.7	per-message-indicators	m	m		see A.1.5/4
1.1.8	per-domain-bilateral-information	o	m-		see A.1.5/5
1.1.9	trace-information	m	m		see A.1.5/6
1.1.10	extensions	m	m		see A.1.6/1
1.1.10.1	recipient-reassignment-prohibited	o	m		
1.1.10.2	dl-expansion-prohibited	o	m		
1.1.10.3	conversion-with-loss-prohibited	o	m		
1.1.10.4	originator-certificate	o	m-		see A.1.5/9
1.1.10.5	message-security-label	o	m-		see A.1.6/3
1.1.10.6	content-correlator	m	m		
1.1.10.7	probe-origin-authentication-check	o	m-		see A.1.6/6
1.1.10.8	internal-trace-information	m	m		see A.1.6/5

Ref	Element	Base	Profile	Support	Notes/References
1.1.10.9	certificate-selectors	o	m-		see A.1.6/9
1.1.10.10	PrivateExtensions	o	o		
1.2	per-recipient-fields	m	m		
1.2.1	recipient-name	m	m		see A.1.7
1.2.2	originally-specified-recipient-number	m	m		
1.2.3	per-recipient-indicators	m	m		
1.2.4	explicit-conversion	o	m-		
1.2.5	extensions	m	m		see A.1.6/1
1.2.5.1	originator-requested-alternate-recipient	o	m-		see A.1.7
1.2.5.2	requested-delivery-method	o	m-		
1.2.5.3	physical-rendition-attributes	o	m-		
1.2.5.4	redirection-history	m	m-		
1.2.5.5	PrivateExtensions	o	o		

A.1.5 Common data types

Ref	Element	Base	Profile	Support	Notes/References
1	MTSIdentifier				
1.1	global-domain-identifier	m	m		see A.1.5/2
1.2	local-identifier	m	m		
2	GlobalDomainIdentifier				
2.1	country-name	m	m		
2.2	administration-domain-name	m	m		
2.3	private-domain-identifier	m	m		
3	EncodedInformationTypes				
3.1	built-in-encoded-information-types	m	m		
3.2	(non-basic parameters)	o	m-		

Ref	Element	Base	Profile	Support	Notes/References
3.3	extended-encoded-information-types	m	m		
4	PerMessageIndicators				
4.1	disclosure-of-other-recipients	m	m		
4.2	implicit-conversion-prohibited	m	m		
4.3	alternate-recipient-allowed	m	m		
4.4	content-return-request	o	m-		
4.5	reserved	o	m-		
4.6	bit-5	o	m-		
4.7	bit-6	o	m-		
4.8	service-message	o	m-		
5	PerDomainBilateralInformation				
5.1	country-name	m	m-		
5.2	administration-domain-name	m	m-		
5.3	private-domain-identifier	o	m-		
5.4	bilateral-information	m	m-		
6	TraceInformation				
6.1	TraceInformationElement	m	m		
6.1.1	global-domain-identifier	m	m		see A.1.5/2
6.1.2	domain-supplied-information	m	m		
6.1.2.1	arrival-time	m	m		
6.1.2.2	routing-action	m	m		
6.1.2.2.1	relayed	m	m		
6.1.2.2.2	rerouted	o	c[1]		
6.1.2.3	attempted-domain	o	c[1]		
6.1.2.4	(additional actions)				
6.1.2.4.1	deferred-time	m	c[2]		

Ref	Element	Base	Profile	Support	Notes/References
6.1.2.4.2	converted-encoded-information-types	o	m-		see A.1.5/3
6.1.2.4.3	other-actions	o	m-		
6.1.2.4.3.1	redirected	o	m-		
6.1.2.4.3.2	dl-operation	o	m-		
7	LastTraceInformation				
7.1	arrival-time	m	m		
7.2	converted-encoded-information-types	m	m		see A.1.5/3
7.3	report-type	m	m		
7.3.1	delivery	m	m		
7.3.1.1	message-delivery-time	m	m		
7.3.1.2	type-of-MTS-user	m	m		
7.3.2	non-delivery	m	m		
7.3.2.1	non-delivery-reason-code	m	m		
7.3.2.2	non-delivery-diagnostic-code	m	m		
8	ContentType				
8.1	built-in	m	m-		
8.2	extended	o	m-		
9	Certificates				
9.1	userCertificate	m	m		see A.1.5/10
9.2	certificationPath	o	m		see A.1.5/10
10	Certificate				
10.1	version	o	m		
10.2	serialNumber	m	m		
10.3	signature	m	m		
10.4	issuer	m	m		

Ref	Element	Base	Profile	Support	Notes/References
10.5	validity	m	m		
10.6	subject	m	m		
10.7	subjectPublicKeyInfo	m	m		
10.8	issuerUniqueIdentifier	o	o		
10.9	subjectUniqueIdentifier	o	o		
10.10	extensions	m	m		
10.10.1	authorityKeyIdentifier	o	o		
10.10.2	subjectKeyIdentifier	o	o		
10.10.3	keyUsage	o	m		
10.10.4	extKeyUsage	o	o		
10.10.5	privateKeyUsagePeriod	o	m		
10.10.6	certificatePolicies	o	m		
10.10.7	policyMappings	o	o		
10.10.8	subjectAltName	o	m		
10.10.8.1	otherName	o	m-		
10.10.8.1.1	mta-name	o	m-		
10.10.8.2	rfc822Name	–	–		
10.10.8.3	dNSName	–	–		
10.10.8.4	x400Address	o	m-		
10.10.8.5	directoryName	o	m-		
10.10.8.6	ediPartyName	–	–		
10.10.8.7	uniformResourceIdentifier	–	–		
10.10.8.8	iPAddress	–	–		
10.10.8.9	registeredID	–	–		
10.10.9	issuerAltName	o	o		
10.10.10	subjectDirectoryAttributes	o	o		
10.10.11	basicConstraints	o	m		

Ref	Element	Base	Profile	Support	Notes/References
10.10.12	nameConstraints	o	o		
10.10.13	policyConstraints	o	o		
10.10.14	cRLDistributionPoints	o	o		
11	CertificateAssertion				
11.1	serialNumber	o	m		
11.2	issuer	o	m		
11.3	subjectKeyIdentifier	o	m		
11.4	authorityKeyIdentifier	o	m		
11.5	certificateValid	o	m		
11.6	privateKeyValid	o	m		
11.7	subjectPublicKeyAlgID	o	m		
11.8	keyUsage	o	m		
11.9	subjectAltName	o	m		
11.10	policy	o	m		
11.11	pathToName	–	–		
1 if rerouting is supported (see A.3.4/2) then m else m- 2 if deferred delivery is supported (see A.3.4/1) then m else m-					

A.1.6 Extension data types

Ref	Element	Base	Profile	Support	Notes/References
1	ExtensionField				
1.1	type	m	m		
1.1.1	standard-extension	m	m		
1.1.2	private-extension	o	m-		see A.3.6
1.2	criticality	m	m		
1.3	value	m	m		
2	MessageOriginAuthenticationCheck				

Ref	Element	Base	Profile	Support	Notes/References
2.1	algorithm-identifier	m	m		
2.2	content	m	m		
2.3	content-identifier	o	m		
2.4	message-security-label	o	m		see A.1.6/3
3	MessageSecurityLabel				
3.1	security-policy-identifier	o	m-		
3.2	security-classification	o	m-		
3.3	privacy-mark	o	m-		
3.4	security-categories	o	m-		
4	MessageToken				
4.1	token-type-identifier	m	m		
4.2	asymmetric-token	m	m		
4.2.1	signature-algorithm-identifier	m	m		
4.2.2	name	m	m		
4.2.3	time	m	m		
4.2.4	signed-data	m	m-		
4.2.4.1	content-confidentiality-algorithm-identifier	o	m-		
4.2.4.2	content-integrity-check	o	m-		
4.2.4.3	message-security-label	o	m-		see A.1.6/3
4.2.4.4	proof-of-delivery-request	o	m-		
4.2.4.5	message-sequence-number	o	m-		
4.2.5	encryption-algorithm-identifier	o	m-		
4.2.6	encrypted-data	o	m-		
4.2.6.1	content-confidentiality-key	o	m-		
4.2.6.2	content-integrity-check	o	m-		
4.2.6.3	message-security-label	o	m-		see A.1.6/3

Ref	Element	Base	Profile	Support	Notes/References
4.2.6.4	content-integrity-key	o	m-		
4.2.6.5	message-sequence-number	o	m-		
5	InternalTraceInformation				
5.1	global-domain-identifier	m	m		
5.2	mta-name	m	m		
5.3	mta-supplied-information	m	m		
5.3.1	arrival-time	m	m		
5.3.2	routing-action	m	m		
5.3.2.1	relayed	m	m		
5.3.2.2	rerouted	o	c[1]		
5.3.3	attempted	o	c[1]		
5.3.3.1	mta	o	m		
5.3.3.2	domain	o	m		
5.3.4	(additional actions)				
5.3.4.1	deferred-time	m	c[2]		
5.3.4.2	converted-encoded-information-types	o	m-		see A.1.5/3
5.3.4.3	other-actions	o	m-		
5.3.4.3.1	redirected	o	m-		
5.3.4.3.2	dl-operation	o	m-		
6	ProbeOriginAuthenticationCheck				
6.1	algorithm-identifier	m	m		
6.2	content-identifier	o	m		
6.3	message-security-label	o	m-		see A.1.6/3
7	ProofOfDelivery				
7.1	algorithm-identifier	m	m		
7.2	delivery-time	m	m		

Ref	Element	Base	Profile	Support	Notes/References
7.3	this-recipient-name	m	m		see A.1.7
7.4	originally-intended-recipient-name	o	m		see A.1.7
7.5	content	m	m		
7.6	content-identifier	o	m		
7.7	message-security-label	o	m-		see A.1.6/3
8	ReportOriginAuthenticationCheck				
8.1	algorithm-identifier	m	m		
8.2	content-identifier	o	m		
8.3	message-security-label	o	m		see A.1.6/3
8.4	per-recipient	m	m		
8.4.1	actual-recipient-name	m	m		
8.4.2	originally-intended-recipient-name	o	m		
8.4.3	delivery	o	m		
8.4.3.1	message-delivery-time	m	m		
8.4.3.2	type-of-MTS-user	m	m		
8.4.3.3	recipient-certificate	o	m		see A.1.5/9
8.4.3.4	proof-of-delivery	o	m		
8.4.3.5	recipient-certificate-selector	o	m		see A.1.5/11
8.4.4	non-delivery	o	m		
8.4.4.1	non-delivery-reason-code	m	m		
8.4.4.2	non-delivery-diagnostic-code	o	m		
9	CertificateSelectors				
9.1	encryption-recipient	o	m-		see A.1.5/11
9.2	encryption-originator	o	m-		see A.1.5/11
9.3	content-integrity-check	o	m-		see A.1.5/11
9.4	token-signature	o	m-		see A.1.5/11

Ref	Element	Base	Profile	Support	Notes/References
9.5	message-origin-authentication	o	m-		see A.1.5/11
10	CertificateSelectorsOverride				
10.1	encryption-recipient	o	m-		see A.1.5/11
10.2	encryption-originator	o	m-		see A.1.5/11
10.3	content-integrity-check	o	m-		see A.1.5/11
10.4	token-signature	o	m-		see A.1.5/11
11	ExtendedCertificate				
11.1	directory-entry	o	m-		
11.2	certificate	o	m		see A.1.5/9
12	ReportingMTAName				
12.1	domain	m	m		see A.1.5/2
12.2	mta-name	m	m		
12.3	mta-directory-name	o	m-		
1 if rerouting is supported then m else m- 2 if deferred delivery is supported then m else m-					

A.1.7 OR-names

Ref	OR-Name Form	Base	Profile	Support	Notes/References
1	mnemonic OR-address	m	m-		see A.1.7.1
2	numeric OR-address	m	m-		see A.1.7.2
3	terminal OR-address	m	m-		see A.1.7.3
4	formatted postal OR-address	m	m-		see A.1.7.4
5	unformatted postal OR-address	m	m-		see A.1.7.5
6	directory-name	o	m-		

The following tables shall be completed according to the OR-address forms for which support is claimed above.

NOTE - Classification of an attribute as m indicates only that its presence is required for the OR-address form, not that the capability to make routing decisions on that attribute is required (see also A.3.1).

A.1.7.1 Mnemonic OR-address

Ref	Element	Base	Profile	Support	Notes/References
1	built-in-standard-attributes	m	m		
1.1	country-name	m	m		
1.2	administration-domain-name	m	m		
1.3	private-domain-name	o	m-		
1.4	organization-name	o	m-		
1.5	personal-name	o	m-		
1.5.1	surname	m	m		
1.5.2	given-name	o	m-		
1.5.3	initials	o	m-		
1.5.4	generation-qualifier	o	m-		
1.6	organizational-unit-names	o	m-		
2	built-in-domain-defined-attributes	o	m-		
3	extension-attributes	o	m-		
3.1	common-name	o	m-		
3.2	teletex-common-name	o	m-		
3.3	universal-common-name	o	m-		see A.1.7.6
3.4	teletex-organization-name	o	m-		
3.5	universal-organization-name	o	m-		see A.1.7.6
3.6	teletex-personal-name	o	m-		
3.6.1	surname	m	m		
3.6.2	given-name	o	m-		
3.6.3	initials	o	m-		
3.6.4	generation-qualifier	o	m-		
3.7	universal-personal-name	o	m-		
3.7.1	surname	m	m		see A.1.7.6
3.7.2	given-name	o	m-		see A.1.7.6

Ref	Element	Base	Profile	Support	Notes/References
3.7.3	initials	o	m-		see A.1.7.6
3.7.4	generation-qualifier	o	m-		see A.1.7.6
3.8	teletex-organizational-unit-names	o	m-		
3.9	universal-organizational-unit-names	o	m-		see A.1.7.6
3.10	teletex-domain-defined-attributes	o	m-		
3.11	universal-domain-defined-attributes	o	m-		see A.1.7.6

A.1.7.2 Numeric OR-address

Ref	Element	Base	Profile	Support	Notes/References
1	built-in-standard-attributes	m	m		
1.1	country-name	m	m		
1.2	administration-domain-name	m	m		
1.3	private-domain-name	o	m-		
1.4	numeric-user-identifier	m	m		
2	built-in-domain-defined-attributes	o	m-		
3	extension-attributes	o	m-		
3.1	teletex-domain-defined-attributes	o	m-		
3.2	universal-domain-defined-attributes	o	m-		see A.1.7.6

A.1.7.3 Terminal OR-address

Ref	Element	Base	Profile	Support	Notes/References
1	built-in-standard-attributes	m	m		
1.1	country-name	o	m-		
1.2	administration-domain-name	o	m-		
1.3	network-address	m	m		
1.4	terminal-identifier	o	m-		
1.5	private-domain-name	o	m-		
1.6	organization-name	o	m-		

Ref	Element	Base	Profile	Support	Notes/References
1.7	personal-name	o	m-		
1.8	organizational-unit-names	o	m-		
2	built-in-domain-defined-attributes	o	m-		
3	extension-attributes	o	m-		
3.1	extended-network-address	m	m		
3.1.1	e163-4-address	o	m-		
3.1.2	psap-address	o	m-		
3.2	terminal-type	o	m-		
3.3	common-name	o	m-		
3.4	teletex-common-name	o	m-		
3.5	universal-common-name	o	m-		see A.1.7.6
3.6	teletex-organization-name	o	m-		
3.7	universal-organization-name	o	m-		see A.1.7.6
3.8	teletex-personal-name	o	m-		
3.9	universal-personal-name	o	m-		see A.1.7.6
3.10	teletex-organizational-unit-names	o	m-		
3.11	universal-organizational-unit-names	o	m-		see A.1.7.6
3.12	unformatted-postal-address	o	m-		
3.13	universal-unformatted-postal-address	o	m-		see A.1.7.6
3.14	teletex-domain-defined-attributes	o	m-		
3.15	universal-domain-defined-attributes	o	m-		see A.1.7.6

A.1.7.4 Formatted postal OR-address

Ref	Element	Base	Profile	Support	Notes/References
1	built-in-standard-attributes	m	m		
1.1	country-name	m	m		
1.2	administration-domain-name	m	m		
1.3	private-domain-name	o	m-		

Ref	Element	Base	Profile	Support	Notes/References
2	extension-attributes	m	m		
2.1	physical-delivery-country-name	m	m		
2.2	physical-delivery-office-name	o	m-		
2.3	universal-physical-delivery-office-name	o	m-		see A.1.7.6
2.4	physical-delivery-office-number	o	m-		
2.5	universal-physical-delivery-office-number	o	m-		see A.1.7.6
2.6	physical-delivery-organization-name	o	m-		
2.7	universal-physical-delivery-organization-name	o	m-		see A.1.7.6
2.8	physical-delivery-personal-name	o	m-		
2.9	universal-physical-delivery-personal-name	o	m-		see A.1.7.6
2.10	postal-code	m	m		
2.11	poste-restante-address	o	m-		
2.12	universal-poste-restante-address	o	m-		see A.1.7.6
2.13	post-office-box-address	o	m-		
2.14	universal-post-office-box-address	o	m-		see A.1.7.6
2.15	pds-name	o	m-		
2.16	street-address	o	m-		
2.17	universal-street-address	o	m-		see A.1.7.6
2.18	unique-postal-name	o	m-		
2.19	universal-unique-postal-name	o	m-		see A.1.7.6
2.20	extension-OR-address-components	o	m-		
2.21	universal-extension-OR-address-components	o	m-		see A.1.7.6
2.22	extension-physical-delivery-address-components	o	m-		
2.23	universal-extension-physical-delivery-address-components	o	m-		see A.1.7.6
2.24	local-postal-attributes	o	m-		

Ref	Element	Base	Profile	Support	Notes/References
2.25	universal-local-postal-attributes	o	m-		see A.1.7.6

A.1.7.5 Unformatted postal OR-address

Ref	Element	Base	Profile	Support	Notes/References
1	built-in-standard-attributes	m	m		
1.1	country-name	m	m		
1.2	administration-domain-name	m	m		
1.3	private-domain-name	o	m-		
2	extension-attributes	m	m		
2.1	unformatted-postal-address	m	m		
2.2	universal-unformatted-postal-address	m	m		see A.1.7.6
2.3	physical-delivery-country-name	m	m		
2.4	postal-code	m	m		
2.5	pds-name	o	m-		

A.1.7.6 UniversalOrBMPString

Ref	Element	Base	Profile	Support	Notes/References
1	UniversalOrBMPString				
1.1	character-encoding				
1.1.1	two-octets	m	m[1]		
1.1.2	four-octets	m	m[1]		
1.2	iso-639-language-code	o	o		

1 this mandatory requirement is to support either alternative character-encoding on origination, and both alternatives on reception.

A.2 Optional functional groups

The following requirements are additional to those specified in A.1 if support of the functional group is claimed (references are to the corresponding table entries in A.1).

A.2.1 Conversion (CV)

A.2.1.1 Operation arguments/results

A.2.1.1.1 MessageTransfer

Ref	Element	Profile
A.1.4.2/1.1.3	original-encoded-information-types	m
A.1.4.2/1.1.4	content-type	m
A.1.4.2/1.2.4	explicit-conversion	c[1]
1 if implicit conversion is not supported (see A.3.3/2) then m else m-		

A.2.1.1.2 ProbeTransfer

Ref	Element	Profile
A.1.4.4/1.1.3	original-encoded-information-types	m
A.1.4.4/1.1.4	content-type	m
A.1.4.4/1.2.4	explicit-conversion	c[1]
1 if implicit conversion is not supported (see A.3.3/2) then m else m-		

A.2.1.2 Common data types

Ref	Element	Profile
A.1.5/6	TraceInformation	
A.1.5/6.1.2.4.2	converted-encoded-information-types	m

A.2.1.3 Extension data types

Ref	Element	Profile
A.1.6/5	InternalTraceInformation	
A.1.6/5.3.4.2	converted-encoded-information-types	m

A.2.2 Distribution List (DL)

A.2.2.1 Operation arguments/results

A.2.2.1.1 MessageTransfer

Ref	Element	Profile
A.1.4.2/1.1.11.6	originator-certificate	c[1]
A.1.4.2/1.1.11.11	dl-expansion-history	m
A.1.4.2/1.1.11.13	certificate-selectors	c[1]
A.1.4.2/1.1.11.14	multiple-originator-certificates	c[1]
A.1.4.2/1.1.11.15	dl-exempted-recipients	c[2]
A.1.4.2/1.2.5.10	message-token	c[1]
A.1.4.2/1.2.5.14	certificate-selectors-override	c[1]
A.1.4.2/1.2.5.15	recipient-certificate	c[3]

1 if DL+SEC or DL+DIR+SEC is claimed then m else m-.

2 if DL+ER is claimed then m else m-.

3 if DL+SEC is claimed then m for reception only otherwise m-.

A.2.2.1.2 ReportTransfer

Ref	Element	Profile
A.1.4.3/1.4.4	reporting-DL-name	m

A.2.2.2 Common data types

Ref	Element	Profile
A.1.5/6	TraceInformation	
A.1.5/6.1.2.4.3	other-actions	m
A.1.5/6.1.2.4.3.2	dl-operation	m
A.1.5/10	Certificate	
A.1.5/10.10.8.4	x400Address	m

A.2.2.3 Extension data types

Ref	Element	Profile
A.1.6/5	InternalTraceInformation	
A.1.6/5.3.4.3	other-actions	m
A.1.6/5.3.4.3.2	dl-operation	m
A.1.6/9	CertificateSelectors	
A.1.6/9.1	encryption-recipient	m
A.1.6/9.4	token-signature	m
A.1.6/10	CertificateSelectorsOverride	
A.1.6/10.1	encryption-recipient	m
A.1.6/10.4	token-signature	m
A.1.6/11	ExtendedCertificate	
A.1.6/11.1	directory-entry	c[1]
1 if DL+DIR+SEC is claimed then m else m-.		

A.2.2.4 OR-names

Ref	OR-Name Form	Profile
A.1.7/6	directory-name	c[1]
1 if DL+DIR or DL+DIR+SEC is claimed then m (for the DL's members) else m-.		

A.2.3 Physical Delivery (PD)

The support requirements specified below are for an MTA with a co-located PDAU. Support of the PD FG on submission is specified in ISO/IEC ISP 10611-4.

A.2.3.1 Operation arguments/results

A.2.3.1.1 MessageTransfer

Ref	Element	Profile
A.1.4.2/1.2.5.5	physical-delivery-modes	m
A.1.4.2/1.2.5.8	physical-rendition-attributes	m

Ref	Element	Profile
A.1.4.2/1.2.5.9	physical-delivery-report-request	m

A.2.3.1.2 ReportTransfer

Ref	Element	Profile
A.1.4.3/2.2.7.2	physical-forwarding-address	m

A.2.3.1.3 ProbeTransfer

Ref	Element	Profile
A.1.4.4/1.2.5.3	physical-rendition-attributes	m

A.2.3.2 OR-names

Ref	OR-Name Form	Profile
A.1.7/4	formatted postal OR-address	m
A.1.7/5	unformatted postal OR-address	m

A.2.3.2.1 Formatted postal OR-address

Ref	Element	Profile
A.1.7.4/2.2	physical-delivery-office-name	m
A.1.7.4/2.3	universal-physical-delivery-office-name	m
A.1.7.4/2.4	physical-delivery-office-number	m
A.1.7.4/2.5	universal-physical-delivery-office-number	m
A.1.7.4/2.6	physical-delivery-organization-name	m
A.1.7.4/2.7	universal-physical-delivery-organization-name	m
A.1.7.4/2.8	physical-delivery-personal-name	m
A.1.7.4/2.9	universal-physical-delivery-personal-name	m
A.1.7.4/2.11	poste-restante-address	m
A.1.7.4/2.12	universal-poste-restante-address	m
A.1.7.4/2.13	post-office-box-address	m
A.1.7.4/2.14	universal-post-office-box-address	m

Ref	Element	Profile
A.1.7.4/2.15	pds-name	m
A.1.7.4/2.16	street-address	m
A.1.7.4/2.17	universal-street-address	m
A.1.7.4/2.18	unique-postal-name	m
A.1.7.4/2.19	universal-unique-postal-name	m
A.1.7.4/2.20	extension-OR-address-components	m
A.1.7.4/2.21	universal-extension-OR-address-components	m
A.1.7.4/2.22	extension-physical-delivery-address-components	m
A.1.7.4/2.23	universal-extension-physical-delivery-address-components	m
A.1.7.4/2.24	local-postal-attributes	m
A.1.7.4/2.25	universal-local-postal-attributes	m

A.2.3.2.2 Unformatted postal OR-address

Ref	Element	Profile
A.1.7.5/2.4	pds-name	m

A.2.4 Redirection (RED)

A.2.4.1 Operation arguments/results

A.2.4.1.1 MessageTransfer

Ref	Element	Profile
A.1.4.2/1.2.5.1	originator-requested-alternate-recipient	m
A.1.4.2/1.2.5.13	redirection-history	m

A.2.4.1.2 ProbeTransfer

Ref	Element	Profile
A.1.4.4/1.2.5.1	originator-requested-alternate-recipient	m
A.1.4.4/1.2.5.4	redirection-history	m

A.2.4.2 Common data types

Ref	Element	Profile
A.1.5/6	TraceInformation	
A.1.5/6.1.2.4.3	other-actions	m
A.1.5/6.1.2.4.3.1	redirected	m

A.2.4.3 Extension data types

Ref	Element	Profile
A.1.6/5	InternalTraceInformation	
A.1.6/5.3.4.3	other-actions	m
A.1.6/5.3.4.3.1	redirected	m

A.2.5 Latest Delivery (LD)

A.2.5.1 Operation arguments/results

A.2.5.1.1 MessageTransfer

Ref	Element	Profile
A.1.4.2/1.1.11.4	latest-delivery-time	m

A.2.6 Return of Content (RoC)

A.2.6.1 Operation arguments/results

A.2.6.1.1 ReportTransfer

Ref	Element	Profile
A.1.4.3/2.1.6	returned-content	m

A.2.6.2 Common data types

Ref	Element	Profile
A.1.5/4	PerMessageIndicators	
A.1.5/4.4	content-return-request	m

A.2.7 Security (SEC)

The support requirements for all SEC security classes are as specified in A.1 unless otherwise specified below. There are no additional requirements for the confidential security class variants (SnC) above those for the primary security classes.

A.2.7.1 Operation arguments/results

A.2.7.1.1 MTABind

Ref	Element	Profile		
		S0	S1	S2
A.1.4.1/1.2.2	initiator-credentials	m	m	m
A.1.4.1/1.2.2.1	simple		i	i
A.1.4.1/1.2.2.2	strong		m	m
A.1.4.1/1.2.2.2.1.4	signed-data		m	m
A.1.4.1/1.2.2.2.2	certificate		c[1]	c[1]
A.1.4.1/1.2.2.2.3	certificate-selector		c[1]	c[1]
A.1.4.1/1.2.3	security-context		m	m
A.1.4.1/2.2.2	responder-credentials	m	m	m
A.1.4.1/2.2.2.1	simple		i	i
A.1.4.1/2.2.2.2	strong		m	m
A.1.4.1/2.2.2.2.1.4	signed-data		m	m
A.1.4.1/2.2.2.2.2	certificate		c[1]	c[1]
A.1.4.1/2.2.2.2.3	certificate-selector		c[1]	c[1]
1 m for reception of each, but only required to be able to generate either certificate or certificate-selector.				

A.2.7.1.2 MessageTransfer

Ref	Element	Profile		
		S0	S1	S2
A.1.4.2/1.1.11.6	originator-certificate			m
A.1.4.2/1.1.11.8	message-origin-authentication-check			m
A.1.4.2/1.1.11.9	message-security-label		m	m
A.1.4.2/1.1.11.13	certificate-selectors			m