INTERNATIONAL STANDARDIZED PROFILE

ISO/IEC ISP 12063-1

Second edition
1997-12-15

Information technology — International Standardized Profiles AMH3n — Message Handling Systems — EDI Messaging —

Part 1:
EDIMG MHS Service Support

Technologies de l'information — Profils normalisés internationaux AMH3n — Systèmes de messagerie — Messagerie EDI —

Partie 1: Support de service EDIMG MHS

Reference number
ISO/IEC ISP 12063-1:1997(E)

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 has created a Special Group on Functional Standardization for the elaboration of 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 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.

International Standardized Profile ISO/IEC ISP 12063-1 was prepared with the collaboration of

— Asia-Oceania Workshop (AOW);

— European Workshop for Open Systems (EWOS);

— Open Systems Environment Implementors' Workshop (OIW).

This second edition cancels and replaces the first edition (ISO/IEC ISP 12063-1:1995), which has been technically revised.

ISO/IEC ISP 12063 consists of the following parts, under the general title *Information technology - International Standardized Profiles AMH3n - Message Handling Systems - EDI Messaging*:

— *Part 1: EDIMG MHS Service Support*

— *Part 2: AMH31 - EDIMG Content*

— *Part 3: AMH32 - EDIMG Requirements for Message Transfer (P1)*

— *Part 4: AMH33 and AMH35 - EDIMG Requirements for MTS Access (P3) and MTS 94 Access (P3)*

— *Part 5: AMH34 - EDIMG Requirements for Enhanced MS Access (P7)*

— *Part 6: AMH36 - EDIMG Requirements for Enhanced MS 94 Access (P7)*

NOTE - Part 6 is not yet published.

Annexes A and B form an integral part of this part of ISO/IEC ISP 12063.
Annexes C, D and E are for information only.

Introduction

This part of ISO/IEC ISP 12063 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 most important roles 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 12063 was 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). This part of ISO/IEC ISP 12063 is harmonized between these three Workshops and it has been ratified by the plenary assemblies of all three Workshops.

This page intentionally left blank

Information technology – International Standardized Profiles AMH3n – Message Handling Systems – EDI Messaging –

Part 1:
EDIMG MHS Service Support

1 Scope

1.1 General

This part of ISO/IEC ISP 12063 contains the overall specifications of the support of MHS Elements of Service and associated MHS functionality in an Electronic Data Interchange Messaging (EDIMG) environment which are generally not appropriate for consideration only from the perspective of a single MHS protocol. These specifications form part of the EDI Messaging application functions, as defined in the parts of ISO/IEC ISP 12063, and are based on the Common Messaging content type-independent specifications in ISO/IEC ISP 10611. Such specifications are in many cases applicable to more than one MHS protocol or are otherwise concerned with component functionality which, although it can be verified via protocol, is not just related to protocol support. They are therefore designed to be referenced in the MHS EDI Messaging application profiles ISO/IEC ISP 12063-2 (AMH31), ISO/IEC ISP 12063-3 (AMH32), ISO/IEC ISP 12063-4 (AMH33 and AMH35), ISO/IEC ISP 12063-5 (AMH34) and ISO/IEC ISP 12063-6 (AMH36) which specify the support of specific MHS protocols and associated functionality.

The specifications in this part of ISO/IEC ISP 12063 are divided into **basic requirements**, which are required to be supported by all EDIMG implementations, and a number of optional **functional groups**, which cover significant discrete areas of related functionality which are not required to be supported by all implementations.

An overview of the scope and applicability of the AMH3n set of profiles and of the structure of this multipart ISP is provided in annex D.

1.2 Position within the taxonomy

This part of ISO/IEC ISP 12063 is the first part, as text common to all parts of the multipart ISP identified in ISO/IEC TR 10000-2 as "AMH3, Message Handling Systems - EDI Messaging".

This part of ISO/IEC ISP 12063 does not, on its own, specify any profiles.

2 Normative references

The following documents contain provisions which, through reference in this text, constitute provisions of this part of ISO/IEC ISP 12063. At the time of publication, the editions indicated were valid. All documents are subject to revision, and parties to agreements based on this part of ISO/IEC ISP 12063 are warned against automatically applying any more recent editions of the documents listed below, since the nature of references made by ISPs to such documents is that they may be specific to a particular edition. Members of IEC and ISO maintain registers of currently valid International Standards and ISPs, and the Telecommunications Standardization Bureau of the ITU maintains a list of currently valid ITU-T Recommendations.

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 12063 to specific clauses of ISO/IEC documents 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 E.

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

ISO/IEC TR 10000-2:—[1], *Information technology - Framework and taxonomy of International Standardized Profiles - Part 2: Principles and Taxonomy for OSI profiles.*

ITU-T Recommendation F.400/X.400 (1996), *Message Handling Systems - System and service overview.*

ISO/IEC 10021-1:—[2], *Information technology - Message Handling Systems (MHS): System and service overview.*

ITU-T Recommendation X.402 (1995) | ISO/IEC 10021-2: 1996, *Information technology - Message Handling Systems (MHS): Overall architecture.*

ITU-T Recommendation X.411 (1995) | ISO/IEC 10021-4: 1997, *Information technology - Message Handling Systems (MHS): Message transfer system: Abstract service definition and procedures.*

ITU-T Recommendation X.413 (1995) | ISO/IEC 10021-5: 1996, *Information technology - Message Handling Systems (MHS): Message store: Abstract service definition.*

ISO/IEC 10021-8: 1995, *Information technology - Message Handling Systems (MHS) - Part 8 : Electronic Data Interchange Messaging Service [see also CCITT Recommendation F.435].*

ISO/IEC 10021-9: 1995, *Information technology - Message Handling Systems (MHS) - Part 9 : Electronic Data Interchange Messaging System [see also CCITT Recommendation X.435].*

ISO/IEC ISP 10611 (all parts), *Information technology - International Standardized Profiles AMH1n - Message Handling Systems - Common Messaging.*

CCITT Recommendation F.435 (1991), *Message handling systems: EDI messaging services.*

CCITT Recommendation X.435 (1991), *Message handling systems: EDI messaging system.*

3 Definitions

For the purposes of this part of ISO/IEC ISP 12063, the following definitions apply.

Terms used in this part of ISO/IEC ISP 12063 are defined in the referenced base standards; in addition, the following terms are defined.

3.1 General

3.1.1 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.

3.1.2 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 interfaces, are outside the scope of this version of ISO/IEC ISP 12063).

---

[1] To be published. (Revision of ISO/IEC 10000:1995)
[2] To be published. (Revision of ISO/IEC 10021-1:1990)

3.2 Support classification

To specify the support level of Elements of Service for this part of ISO/IEC ISP 12063, the following terminology is defined.

3.2.1 mandatory support (m):

for origination:

for MT and MS Elements of Service:

A service provider (i.e. an MTA or MS) shall be able to make the Element of Service available to a service user in the role of originator; a service user (i.e. a UA) shall be able to use the Element of Service in the role of originator.

for EDI Elements of Service:

A service provider (i.e. an EDI-UA) shall implement all the procedures specified in the base standards which are associated with the provision of the Element of Service, including use of the corresponding MT or MS Element(s) of Service, as appropriate; where specified in the base standards, a service provider shall make the Element of Service available to the service user in the role of originator; in all cases, it shall be stated in the PICS whether the Element of Service is made available to the service user and, if so, how this is achieved.

for reception:

for MT and MS Elements of Service:

A service provider (i.e. a MTA or MS) shall be able to make the Element of Service available to a service user in the role of recipient; a service user (i.e. a UA) shall be able to use the Element of Service in the role of recipient.

for EDI Elements of Service:

A service provider (i.e. an EDI-UA) shall implement all the procedures specified in the base standards which are associated with the provision of the Element of Service, including use of the corresponding MT or MS Element(s) of Service, as appropriate; where specified in the base standards, a service provider shall make the Element of Service available to the service user in the role of recipient; in all cases, it shall be stated in the PICS whether the Element of Service is made available to the service user and, if so, how this is achieved.

3.2.2 optional support (o): An implementation is not required to support the Element of Service. If support is claimed, then the Element of Service shall be treated as if it were specified as mandatory support.

3.2.3 conditional support (c): The Element of Service shall be supported under the conditions specified in this part of ISO/IEC ISP 12063. If these conditions are met, the Element of Service shall be treated as if it were specified as mandatory support. If these conditions are not met, the Element of Service shall be treated as if it were specified as optional support (unless otherwise stated).

3.2.4 out of scope (i): The Element of Service is outside the scope of this part of ISO/IEC ISP 12063 - i.e. it will not be the subject of an ISP conformance test. However, the handling of associated protocol elements may be specified separately in the subsequent parts of ISO/IEC ISP 12063.

3.2.5 not applicable (–): The Element of Service is not applicable in the particular context in which this classification is used.

3.3 Profile object identifiers

Profiles that are specified in ISO/IEC ISP 12063 are identified by the object identifiers in table 1.

NOTE - These object identifiers are included for formal purposes and any use of them is not defined. They are not related to any implementation of messaging and do not appear in the protocols specified in ISO/IEC ISP 12063.

Table 1 - Profile object identifiers

Profile	Object Identifier
AMH31	{ iso standard edi-messaging(12063) edimg-content(2) }
AMH32	{ iso standard edi-messaging(12063) edimg-message-transfer(3) }
AMH33	{ iso standard edi-messaging(12063) edimg-mts-access(4) }
AMH34	{ iso standard edi-messaging(12063) edimg-ms-access(5) }
AMH35	{ iso standard edi-messaging(12063) edimg-mts-94-access(6) }
AMH36	{ iso standard edi-messaging(12063) edimg-ms-94-access(7) }

4 Abbreviations

84IW	84 Interworking
AF	Automatic Forwarding
ASN.1	Abstract Syntax Notation One
CV	Conversion
DC	Delivery Constraints
DIR	Use of Directory
DL	Distribution List
EDI	Electronic data interchange
EDI-MS	EDI message store
EDI-UA	EDI user agent
EDIFACT	EDI For Administration, Commerce and Transport
EDIM	EDI Message
EDIMG	EDI Messaging
EDIN	EDI Notification
EH	EDIFACT Heading fields
EIT	Encoded information type
EoS	Element of Service
FG	Functional group
FN	Forwarded notification
IPM	Interpersonal message or Interpersonal messaging
ISP	International Standardized Profile
ISPICS	International Standard Protocol Implementation Conformance Statement
LD	Latest Delivery
MF	Manual Forwarding
MHS	Message Handling Systems
MPB	Multi part body
MS	Message store
MT	Message transfer
MTA	Message transfer agent
MTS	Message Transfer System
NN	Negative notification
OSI	Open Systems Interconnection
PD	Physical Delivery
PDAU	Physical delivery access unit
Pedi	Protocol for electronic data interchange
PN	Positive notification
PS	Private syntax
RED	Redirection

RED2	Redirection Instructions
RD	Restricted Delivery
SEC	Security
UA	User agent
SPP	Simple Protected Password
X12	ANSI X12

Support level for Elements of Service (see 3.2):

m	mandatory support
o	optional support
c	conditional support
i	out of scope
–	not applicable

5 Conformance

No conformance requirements are specified in this part of ISO/IEC ISP 12063.

NOTE - This part of ISO/IEC ISP 12063 is a reference specification of the basic requirements and functional groups covered by the AMH3n set of profiles and is additional to the protocol-specific requirements specified in the following parts of ISO/IEC ISP 12063. Although this part of ISO/IEC ISP 12063 contains normative requirements, there is no separate conformance to this part (i.e. it is not identified in the MHS taxonomy in ISO/IEC TR 10000-2) since such requirements are only significant when referenced in the context of a particular protocol.

Conformance requirements are specified by protocol for each MHS functional object in the following parts of ISO/IEC ISP 12063 with reference to the specifications in this part. Support of functionality as specified in this part may only be verifiable where the effect of implementation can be determined at a standardized external interface - i.e. via a standard OSI communications protocol. Further, the provision of Elements of Service and other functionality at a service interface will not necessarily be verifiable unless such interface is realized in the form of a standard OSI communications protocol. Other forms of exposed interface (such as a human user interface or a standardized programmable interface may be provided, but are not required for conformance to this version of ISO/IEC ISP 12063.

6 Basic requirements

Annex A specifies the basic requirements for support of MHS Elements of Service (EoS) for conformance to ISO/IEC ISP 12063. Basic requirements specify the level of support required by all EDIMG implementations, as relevant to each type of MHS functional object - i.e. MTA, MS or UA (as MTS-user or MS-user, as relevant).

An implementation conforming to the basic requirements of ISO/IEC ISP 12063 shall conform to the basic requirements of ISO/IEC ISP 10611, as appropriate to the type of MHS functional object.

6.1 Generation of notifications

An EDI-UA implementation shall be able to accept or refuse EDI responsibility for a received EDIM. It shall be able to generate appropriate positive and negative EDI notifications to respond to EDI notification requests, either locally or by request from the EDIMG user as defined in the MHS base standards. The error codes are generated either by the EDIMG user or by the EDI-UA.

It shall be stated in the PICS which EDIN reason code values an EDI-UA implementation is able to generate.

6.2 Reception of notifications

An EDI-UA shall be able to receive any type of EDI notification.

6.3 Number of recipients

If an EDI-UA implementation comprises any limit on the number of recipients that can be specified in an EDIM heading, then such limit shall be stated in the PICS.

6.4 Message length

If an EDI-UA implementation imposes any constraint on the size of the message content, then such constraint shall be stated in the PICS.

6.5 Identification of the recipient

The originating EDI-UA shall use the same OR-name in the RecipientField as in the Submission envelope.

On reception of an EDIM, the EDI-UA shall identify its own recipient sub-fields in the EDIM heading fields based on OR-name in the RecipientField in the RecipientsSubField of the EDIM. The value shall be the OR-name from the first element in the redirection-history argument (if present) or else the this-recipient-name argument of the Message Delivery operation.

NOTES

1 - Where the EDIM passes through intermediate MTAs implementing X.400 (84) after a redirection, a bilateral agreement will be needed since the redirection-history is lost.

2 - Where the EDIM has been delivered as a result of DL expansion, the EDI-UA can not identify its own recipient sub-fields.

3 - The requirements in this clause are also submitted to ITU-T and ISO/IEC as a perceived defect in the base standard.

6.6 Body part types and encoded information types

It shall be stated in the PICS which body part types and encoded information type values an implementation supports in the roles of originator and receiver. An MTA or an MS implementation shall be able to accept any syntax.

The use of PRIVATE and UNDEFINED EDI body part types is deprecated in favour of privately defining an object identifier for the specific syntax used (see 7.12).

7 Functional groups

Annex A specifies any additional requirements for support of MHS EoS if support of an optional functional group (FG) is claimed, as appropriate to each type of MHS functional object. The following clauses summarize the functionality supported by each of the optional FGs and identify any particular such requirements or implementation considerations which are outside the scope of formal conformance to ISO/IEC ISP 12063. A summary of the functional groups, identifying which may be supported (Y) and which are not applicable (N) for each type of MHS functional object (i.e. MTA, MS or UA - whether as MTS-user or as MS-user is not distinguished), is given in table 2.

The conformance requirements for support of the various functional groups, covering support of additional protocol elements and/or procedures, are specified in parts 2, 3, 4, 5 and 6 of ISO/IEC ISP 12063, according to the protocol(s) to which each functional group relates.

Table 2 - Summary of AMH3n optional functional groups

Functional Group	Inheritance from AMH1n	relevant to a MTA	relevant to a MS	relevant to a UA
EDI Conversion (CV) [1]	inherited	Y	N	N
EDI Distribution List (DL) [1]	inherited	Y	N	N
EDI Physical Delivery (PD) [1]	inherited	Y	N	Y
EDI Forwarding (AF, MF)	new	N	Y	Y
EDI Redirection (RED) [1]	inherited	Y	N	Y
EDI Latest Delivery (LD) [1]	inherited	Y	N	Y
EDI Security (SEC1, SEC2, SEC3) (S0, S0C) [2] (S1, S1C, S2, S2C) [2]	 new inherited inherited	 N N Y	 Y Y Y	 Y Y Y
EDI Use of Directory (DIR) [1]	inherited	Y	N	Y
EDI 84 Interworking (84IW) [2]	inherited	Y	N	Y
EDI Multi-Part Body (MPB)	new	N	Y	Y
EDI ANSI X12 (X12)	new	N	N	Y
EDI Private Syntax (PS)	new	N	N	Y
EDI EDIFACT Heading fields (EH)	new	N	Y	Y
EDI Simple Protected Password (SPP) [1]	inherited	Y	Y	Y
EDI Redirection Instructions (RED2) [1]	inherited	Y	N	Y
EDI Delivery Constraints (DC) [1]	inherited	Y	N	Y
EDI Restricted Delivery (RD) [1]	inherited	Y	N	Y

1 There are no additional requirements to those specified in ISO/IEC ISP 10611.
2 Further requirements to those in ISO/IEC ISP 10611 are specified.

7.1 EDI Conversion (CV)

No explicit conversions have been defined for the primary body part (which contains an EDI body part or EDIM body part) by the MTS. Implicit conversion of the primary body part is permitted, but the specification of particular conversions is beyond the scope of ISO/IEC ISP 12063.

Implicit or explicit conversion of other body parts (which contain additional information, such as graphics or text) shall conform to the Common Messaging Conversion FG specified in ISO/IEC ISP 10611. Any such conversions performed by the receiving EDI-UA are outside the scope of ISO/IEC ISP 12063.

NOTE -The use of some MHS security EoS require that any conversion that is performed by the receiving EDI-UA must be done after the security services are performed.

7.2 EDI Distribution List (DL)

The EDI Distribution List FG covers all issues relating to the performance of distribution list (DL) expansion.

An implementation conforming to the EDI DL FG shall conform to the Common Messaging DL FG as specified in ISO/IEC ISP 10611. There are no additional requirements for an MTA in an EDIMG environment.

7.3 EDI Physical Delivery (PD)

The EDI Physical Delivery FG is concerned with access to physical delivery (i.e. postal, courier, etc.) services. The EDI PD FG comprises two separate and distinct parts:

support of PD EoS on origination and submission;

support of a co-located physical delivery access unit (PDAU).

Support of PD EoS on submission may be relevant either for an EDI-UA or an MTA. Support of a PDAU is only applicable to an MTA. The requirements for the PDAU itself are outside the scope of ISO/IEC ISP 12063

An implementation conforming to the EDI PD FG shall conform to the Common Messaging PD FG as specified in ISO/IEC ISP 10611. An EDI-UA conforming to the EDI PD FG shall also make the PD EoS available to the EDIMG user for origination as specified in ISO/IEC ISP 10611. There are no additional requirements for the MTA in an EDIMG environment.

7.4 EDI Forwarding (AF, MF)

The EDI Forwarding FG defines the service and functionality required to perform forwarding of EDIMs by or on behalf of an EDIMG user.

The EDI Forwarding FG is specified as two classes: Automatic Forwarding (AF) and Manual Forwarding (MF). In class AF the forwarding is performed automatically by the EDI-UA or by the EDI-MS based on a set of criteria specified by the EDIMG-user. The available criteria and their invocation method shall be stated in the PICS. In class MF the forwarding is performed by the EDI-UA on explicit instruction by the EDIMG-user on each occasion.

It shall be stated in the PICS whether or not removal of body parts is supported.

NOTE - The MHS base standards requires that support of the notifications and information fields associated with forwarding (i.e. those mandated in this FG) is mandatory if forwarding is performed.

7.4.1 EDI Forwarding class (AF)

The EDI Automatic Forwarding class (AF) supports use of the Stored EDI Message Auto-forward EoS.

7.4.2 EDI Forwarding class (MF)

The EDI Manual Forwarding class (MF) supports use of the EDI Forwarding EoS by an EDI-UA.

7.5 EDI Redirection (RED

The EDI Redirection FG covers support of those EoS which provide the functionality required to perform the actions associated with the delivery of a message to a recipient other than the one initially specified by the originator.

An MTA implementation conforming to the EDI RED FG shall conform to the Common Messaging RED FG as specified in ISO/IEC ISP 10611. There are no additional requirements for an MTA in an EDIMG environment.

7.6 EDI Latest Delivery (LD)

The EDI Latest Delivery FG covers support of the Latest Delivery EoS - i.e. the functionality required to cause non-delivery to occur if a latest delivery time specified by the originator has expired.

An implementation conforming to the EDI LD FG shall conform to the Common Messaging LD FG as specified in ISO/IEC ISP 10611. There are no additional requirements for an MTA or EDI-UA in an EDIMG environment.

7.7 EDI Security (SEC1, SEC2, SEC3, S0, S0C, S1, S1C, S2, S2C)

The EDI Security FG covers the provision of security service in an EDIMG environment. As the interface between the EDIMG user and the EDI-UA is outside the scope of this profile, implementations of security mechanisms can be in the EDI-UA or as part of a general security mechanism integrated with the EDIMG user object.

The EDI Security FG is specified as three independent **security classes** denoted as SEC1, SEC2 and SEC3. In addition to this, an EDIMG implementation can support any of the Common Messaging security classes S0, S0C, S1, S1C, S2 and S2C.

An implementation claiming conformance to the EDI Security FG shall state which security class(es) are supported.

The security classes SEC1 and SEC2 require support of the Content Integrity EoS. SEC2 also requires support of the Message Origin Authentication EoS. This may be achieved by supporting Common Messaging security class S0 as specified in ISO/IEC ISP 10611 (see 7.7.2).

NOTE - A separate Functional Group is defined for Simple Protected Password, since it was introduced in the base standard in the 1995-1996 publication.

7.7.1 EDI specific security classes (SEC1, SEC2, SEC3)

The EDI Security FG supports use of EDIMG security services and functionality provide within the EDIMs and EDINs as follows :

Table 3 - EDI Security Classes

Element of Service	Security Class		
	SEC1	SEC2	SEC3
Application Security Element	o	o	m
Non-repudiation of Content Originated	o	m	o
Non-repudiation of Content Received	o	m	o
Non-repudiation of Content Received Request	o	m	o
Non-repudiation of EDI Notification	o	m	o
Non-repudiation of EDI Notification Request	o	m	o
Proof of Content Received	m	m	o
Proof of Content Received Request	m	m	o
Proof of EDI Notification	m	m	o
Proof of EDI Notification Request	m	m	o

Security class SEC1 requires that security measures shall be provided by the EDIMG system implementation in order to provide EDI-UA to EDI-UA proof services for an EDIMs.

Security class SEC2 requires that security measures shall be provided by the EDIMG system implementation in order to provide EDI-UA to EDI-UA non-repudiation services for an EDIMs.

Security class SEC3 requires that security measures shall be provided by the EDIMG system implementation in order to provide EDIMG user to EDIMG user security services.

7.7.2 Common messaging security (S0, S0C, S1, S1C, S2, S2C)

The Common messaging Security classes covers the provision of secure messaging in an EDIMG environment and is specified as three **security classes** which are incremental subsets of the security features available in the MHS base standards:

S0 This security class only requires security functions which are applicable between MTS-users. Consequently security mechanisms are implemented within the MTS-user. An MTA is only required to support the syntax of the security services on submission and delivery (support of the syntax on relaying is a basic requirement). An MTA is not expected to understand the semantics of the security services.

S1 This security class requires security functionality within both the MTS-user and the MTS. The MTS security functionality is only required to achieve secure access management. As with S0, most of the security mechanisms are implemented within an MTS user. S1 primarily provides integrity and authentication between MTS users. However, MTAs are expected to support digital signatures for peer-to-peer authentication, security labelling and security contexts.

S2 This security class adds security functions within MTAs and the MTS. The main security function added within this class is authentication within the MTS, and hence non-repudiation can also be provided.

In addition, each of the three security classes has a variant (denoted as **S0C**, **S1C** and **S2C**) which requires support of end-to-end content confidentiality.

The requirements for an implementation conforming to the Common Messaging security classes are specified in ISO/IEC ISP 10611. There are no additional requirements for an MTA, UA or MS in an EDIMG environment.

7.8 EDI Use of Directory (DIR)

The EDI Use of Directory FG covers support of the Designation of Recipient by Directory Name EoS as follows:

- support of specification of a recipient by means of a directory name by an MTS-user or an MTA on submission;
- support of access to a directory service by an MTA to obtain one or more OR-addresses (either on submission or subsequently if an OR-address is absent or determined to be invalid and a directory name is present).

An implementation conforming to the EDI DIR FG shall conform to the Common Messaging DIR FG as specified in ISO/IEC ISP 10611. There are no additional requirements for an MTA or UA.

NOTES

1 - A directory may also be used directly by MHS users to obtain information to assist in the submission of messages. However, such use is not necessarily MHS-specific and is therefore outside the scope of ISO/IEC ISP 12063.

2 - There are FDI2 profiles currently under development which will describe directory attributes and their usage by MHS.

7.9 EDI 84 Interworking (84IW)

The 84 Interworking FG covers interworking between implementations conforming to ISO/IEC ISP 12063 (hereafter referred to as '1988 systems') and implementations conforming to the CCITT X.400(1984) Recommendations (hereafter referred to as '1984 systems').

An MTA implementation conforming to the EDI 84IW FG shall conform to the Common Messaging 84IW FG as specified in ISO/IEC ISP 10611. There are no additional requirements for an MTA in an EDIMG environment.

A UA implementation conforming to the EDI 84IW FG shall support origination and reception of IPM content identified as integer 2 as specified in subclause 20.2 of ISO/IEC 10021-7 and shall support origination and reception of IA5 Text body part.

Additional recommended practices for interworking with earlier EDI messaging implementations are described in annex C.

7.10 EDI Multi-Part Body (MPB)

The EDI Multi-Part Body FG defines the service and functionality that is required to support the generation of multiple body parts in an EDIM.

7.11 EDI ANSI X12 (X12)

The EDI ANSI X12 FG covers support of the ANSI X12 EDI syntax, including conveyance of an X12 interchange within the EDI body part. Support of the applicable X12 heading fields is also required.

7.12 EDI Private syntax (PS)

The EDI Private syntax FG covers support of all possible privately defined EDI syntaxes. It includes conveyance of a privately defined object identifier, identifyng the interchange syntax within the EDI body part (i.e. object identifiers not defined in the base standard). See further subclause 8.2.6 of ISO/IEC 10021-9.

Support can be claimed by an implementation which passes the interchange transparently to the EDIMG-user.

7.13 EDI EDIFACT heading fields (EH)

The EDI EDIFACT heading fields FG covers support of the handling of EDIFACT heading field data elements of the EDI interchange, in the corresponding EDIM heading fields.

NOTE - edi-message-type is covered in the basic requirement to ISO/IEC ISP 12063.

It shall be stated for origination and for reception in the PICS, whether the EDI-UA checks for the semantic equivalence of elements common to the EDI information in the EDI body part and the EDIM header.

7.14. EDI Simple Protected Password (SPP)

The EDI Simple Protected Password FG covers all issues relating to the handling of the simple protected password authentication introduced in the P3 and P7 contexts, in the 1995-1996 publication of the base standards.

An implementation conforming to the EDI SPP FG shall conform to the Common Messaging SPP FG as specified in ISO/IEC ISP 10611. There are no additional requirements for an MTA, MS or UA in an EDIMG environment.

7.15. EDI Redirection instructions (RED2)

The EDI Redirection Instructions FG covers support of the registration of additional conditions for redirection of messages (e.g. maximum content length, acceptable eits and priority).

An implementation conforming to the EDI Redirection Instructions FG shall conform to the Common Messaging RED2 FG as specified in ISO/IEC ISP 10611. There are no additional requirements for an MTA or UA in an EDIMG environment.

7.16. EDI Delivery constraints (DC)

The EDI Delivery Constraints FG covers support of the enhansed functionality for the recipient to defined constraints on the delivery to him (e.g. maximum content length, acceptable eits and unacceptable eits).

An implementation conforming to the EDI Delivery Constraints FG shall conform to the Common Messaging DC FG as specified in ISO/IEC ISP 10611. There are no additional requirements for an MTA or UA in an EDIMG environment.

7.17. EDI Restricted Delivery (RD)

The EDI Restricted Delivery FG covers support of the enhansed functionality for the originator to defined constraints on the delivery to the recipient (e.g. whether a specified OR-address is permitted or not).

An implementation conforming to the EDI Restricted Delivery FG shall conform to the Common Messaging RD FG as specified in ISO/IEC ISP 10611. There are no additional requirements for an MTA or UA in an EDIMG environment.

8 Naming and addressing

Implementations shall support naming and addressing capabilities as specified in clause 8 of ISO/IEC ISP 10611-1.

In addition, an EDI-UA implementation shall support use of the numeric and terminal forms to identify recipients. Use of these forms to identify the EDI-UA itself is not required.

9 Error and exception handling

The upper bounds defined in annex G of ISO/IEC 10021-9 are normative for the purposes of ISO/IEC ISP 12063.

An implementation shall not generate elements which exceed such bounds.

An implementation detecting a violation of such bounds may generate a size-constraint-violation, but is not required to do so.

An implementation is not required to be able to accept elements up to such bounds where an appropriate error indication is defined in the base standards.

Annex A

(normative)

Elements of Service

In the event of a discrepancy becoming apparent in the body of this part of ISO/IEC ISP 12063 and the tables in this annex, this annex is to take precedence.

A.1 MT Elements of Service

The requirements for support of MT EoS by an MTA are as specified in clause A.1 of ISO/IEC ISP 10611-1. The following tables specify the requirements for use of such services by an MTS-user in an EDIMG environment (i.e. EDI-UA) for conformance to ISO/IEC ISP 12063. Whether such services are made available to the MHS user is covered in the AMH31 PICS proforma.

In the following tables, the "Basic" column reflects the basic requirements for conformance to ISO/IEC ISP 12063 - i.e. the minimum level of support required by all EDI-UA implementations (see clause 6). The "Functional Group" column specifies any additional support requirements if support of an optional functional group is claimed (see clause 7). Each column is then further subdivided into support for origination ("Orig") and reception ("Rec") as defined in 3.2, together with the abbreviated name of the functional group ("FG") in the case of the second column.

Table A.1 - Elements of Service Belonging to The Basic EDIMG Service (MT EoS)

Element of Service	Basic		Functional Group		
	Orig.	Rec.	FG	Orig.	Rec.
Access Management	m	m			
Content Type Indication	m	m			
Converted Indication	–	m			
Delivery Time Stamp Indication	–	m			
Message Identification	m	m			
Non-delivery Notification	m	–			
Original Encoded Information Types Indication	m	m			
Submission Time Stamp Indication	m	m			
User/UA Capabilities Registration	–	m			

Table A.2 - EDIMG Optional User Facilities (MT EoS)

Element of Service	Basic		Functional Group		
	Orig.	Rec.	FG	Orig.	Rec.
Additional Physical Rendition	o	–			
Alternate Recipient Allowed	m	–			
Alternate Recipient Assignment[1]	–	–			
Basic Physical Rendition	o	–	PD	m	
Content Confidentiality	o	o	S0C S1C S2C	m m m	m m m
Content Integrity	o	o	S0 SEC1 SEC2	m m m	m m m
Conversion Prohibition	m	m			
Conversion Prohibition in Case of Loss of Information	o	o			
Counter Collection	o	–	PD	m	
Counter Collection with Advice	o	–			
Deferred Delivery	m	–			
Deferred Delivery Cancellation	m[2]	–			
Delivery Notification	m	–			
Delivery via Bureaufax Service	o	–			
Designation of Recipient by Directory Name	o	–	DIR	m	
Disclosure of Other Recipients	m	m			
DL Expansion History Indication	–	m			
DL Expansion Prohibited	m[3]	–			
EMS (Express Mail Service)	o	–	PD	m	
Explicit Conversion	o	–			
Grade of Delivery Selection	m	m			
Hold for Delivery	–	o			
Implicit Conversion	–	–			
Latest Delivery Designation	o	–	LD	m	

Element of Service	Basic		Functional Group		
	Orig.	Rec.	FG	Orig.	Rec.
Message Flow Confidentiality	i	i			
Message Origin Authentication	o	o	S0 SEC1 SEC2	m m m	m m m
Message Security Labelling	o	o	S1	m	m
Message Sequence Integrity	o	o			
Multi-destination Delivery	m	–			
Non-repudiation of Delivery	o	o	S2	m	m
Non-repudiation of Origin	o	o	S2	m	m
Non-repudiation of Submission	i	–	S2	m	m
Ordinary Mail	o	–	PD	m	
Originator Requested Alternate Recipient	o	–	RED	m	
Physical Delivery Notification by MHS	o	–			
Physical Delivery Notification by PDS	o	–			
Physical Forwarding Allowed	o	–	PD	m	
Physical Forwarding Prohibited	o	–	PD	m	
Prevention of Non-delivery Notification	o	–			
Probe	o	–			
Probe Origin Authentication	i	–			
Proof of Delivery	o	o	S1	m	m
Proof of Submission	i	–	S2	m	m
Redirection Disallowed by Originator	m[4]	–			
Redirection of Incoming Messages	–	o	RED		m[5]
Registered Mail	o	–			
Registered Mail to Addressee in Person	o	–			
Report Origin Authentication	i	i	S2	m	m
Request for Forwarding Address	o	–			

Element of Service	Basic		Functional Group		
	Orig.	Rec.	FG	Orig.	Rec.
Requested Preferred Delivery Method	o	o			
Restricted Delivery	–	i			
Return of Content	i	–			
Secure Access Management	o	o	S1	m	m
Special Delivery	o	–	PD	m	
Undeliverable Mail with Return of Physical Message	o	–	PD	m	
Use of Distribution List	m[6]	–			

1 The method by which an alternate recipient is specified to the MTA is outside the scope of ISO/IEC ISP 12063 .

2 Performance of this EoS is not guaranteed if the message has already been transferred from the submitting MTA.

3 To prevent an unknown number of EDINs from being sent to the original originator of an EDIM in the case of DL-expansion, "DL-expansion-prohibited" should normally to be set to "prohibited" any of PN, NN or FN is requested..

4 Support of this Elements of Service has been made mandatory as the default is "allowed". Only the capability to generate the "prohibited" value is required for conformance.

5 It is not required that the support of this EoS is achieved using the Register operation.

6 Use of Distribution List on submission is always possible as DLs cannot be distinguished from other OR-addresses.

A.2 MS Elements of Service

The requirements for support of MS EoS by an MS are as specified in clause A.2 of ISO/IEC ISP 10611-1 except as modified table A.4. The following tables specify the requirements for use of such services by an EDI-MS-user in an EDIMG environment (i.e. EDI-UA) for conformance to ISO/IEC ISP 12063. Whether such services are made available to the MHS user is covered in the AMH31 PICS proforma.

In the following tables, the "Basic" column reflects the basic requirements for conformance to ISO/IEC ISP 12063 - i.e. the minimum level of support required by all EDI-UA implementations (see clause 6). The "Functional Group" column specifies any additional support requirements if support of an optional functional group is claimed (see clause 7), together with the abbreviated name of the functional group ("FG").

Table A.3 - Base EDI Message Store Facilities

Element of Service	Basic		Functional Group		
	Orig.	Rec.	FG	Orig.	Rec.
MS Register	o	o	AF	m	m
Stored Message Deletion	m	m			
Stored Message Fetching	m	m			
Stored Message Listing	o	o			
Stored Message Summary	o	o			

Table A.4 - EDI Message Store Optional User Facilities

Element of Service	Basic		Functional Group		
	Orig.	Rec.	FG	Orig.	Rec.
Stored Message Alert	o	o			
Stored Message Auto-forward	i	i			
Stored EDI Message Auto-forward	o	o	AF	m	m

A.3 EDIMG-specific Elements of Service

The following tables specify the requirements for support of EDIMG-specific Elements of Service by an MTS-user in an EDIMG environment (i.e. EDI-UA) for conformance to ISO/IEC ISP 12063. Whether such services are made available to the MHS user is covered in the AMH31 PICS proforma.

In the following tables, the "Basic" column reflects the basic requirements for conformance to ISO/IEC ISP 12063 - i.e. the minimum level of support required by all EDI-UA implementations (see clause 6). The "Functional Group" column specifies any additional support requirements if support of an optional functional group is claimed (see clause 7). Each column is then further subdivided into support for origination ("Orig") and reception ("Rec") as defined in 3.2, together with the abbreviated name of the functional group ("FG") in the case of the second column.

Table A.5 - Elements of Service Belonging to The Basic EDIMG Service (EDIMG EoS)

Element of Service	Basic		Functional Group		
	Orig.	Rec.	FG	Orig.	Rec.
EDI Message Identification	m	m			
Typed Body	m	m			

Table A.6 - EDIMG Optional User Facilities (EDIMG EoS)

Element of Service	Basic		Functional Group		
	Orig.	Rec.	FG	Orig.	Rec.
Application Security Element	o	o	SEC3	m	m
Character Set	m	m			
Cross Reference Information	o	m	MPB	m	
EDI Forwarding	o	–	AF, MF	m	
EDI Message Type(s)	m	m			
EDI Notification Request	m	m			
EDI Standard Indication	m	m			
EDIM Responsibility Forwarding Allowed Indication	m	m			
EDIN Receiver	o	m	AF, MF	m	
Expiry Date/Time Indication	o	m			
Incomplete Copy Indication	o	m	AF, MF	c[1]	
Interchange Header	m	m			
Multi-part Body	o	m	MPB	m	

Element of Service	Basic		Functional Group		
	Orig.	Rec.	FG	Orig.	Rec.
Non-repudiation of Content Originated	o	o	SEC2	m	m
Non-repudiation of Content Received	o	o	SEC2	m	m
Non-repudiation of Content Received Request	o	o	SEC2	m	m
Non-repudiation of EDI Notification	o	o	SEC2	m	m
Non-repudiation of EDI Notification Request	o	o	SEC2	m	m
Obsoleting Indication	o	m[2]			
Originator Indication	m	m			
Proof of Content Received	o	o	SEC1 SEC2	m m	m m
Proof of Content Received Request	o	o	SEC1 SEC2	m m	m m
Proof of EDI Notification	o	o	SEC1 SEC2	m m	m m
Proof of EDI Notification Request	o	o	SEC1 SEC2	m m	m m
Recipient Indication	m	m			
Related Message(s)	o	m			
Services Indication	o	o			

1 Support on origination is conditional on supporting removal of body parts.

2 The EDI-UA do not has any control when the EDIM is transferred to the EDIMG user.

Annex B

(normative)

Amendments and corrigenda

International Standards are subject to constant review and revision by the ISO/IEC Technical Committees concerned. The following amendments and corrigenda are approved by ISO/IEC JTC1 and ITU-T SG 7 and are considered as normative references in this part of ISO/IEC ISP 12063.

ISO/IEC 10021-2:1996/Cor.1:1997

ISO/IEC 10021-4:1997/Cor.1:1997

ISO/IEC 10021-5:1996/Cor.1:1997

ISO/IEC 10021-9:1995/Cor.1:1997

Annex C

(informative)

Additional recommended practices for 1984 interworking

C.1 Introduction

This annex provides some additional recommendations concerning interworking between EDI-UA implementations according to ISO/IEC ISP 12063 (hereafter referred to as '1988 systems') and UA implementations according to earlier recommended practices (hereafter referred to as '1984 systems').

These recommended practices are additional to the requirements of the EDI 84 Interworking functional group, either because the interworking issue in question is outside the scope of the MHS base standards (and hence also outside the scope of formal conformance to ISO/IEC ISP 12063) or because it is anticipated that the issue should be resolved in the MHS base standards.

The recommendations in this annex are concerned with the downgrading of EDIMs (content type 35) into interpersonal messages (content type 2). Such a capability could be implemented in an originating EDI-UA or elsewhere in the message path.

This annex does not specify the conditions under which an implementation may invoke these procedures, or how a requirement for downgrading of a particular EDIM should be determined. Such determination will require knowledge of the recipient's capabilities, bilateral agreements, configuration or some other appropriate means. Without such knowledge it may be inappropriate to invoke these procedures, and it is strongly recommended that content downgrading is only performed when it is known that it is appropriate to do so.

NOTE - Recommended practices for interworking between 1988 and 1984 MTA implementations are covered in annex D of ISO/IEC ISP 10611-1.

There are different scenarios for interworking with 1984 systems. These are:

- interworking between an EDIMG user and a 1984 MTA;
- interworking between EDIMG systems and IPM systems.

In a global messaging environment it is conceivable that an EDI-UA may be involved in all scenarios with different parties.

The case of an EDI-UA forwarding EDIMs between a 1984 EDIMG system and a 1988 EDIMG system is not considered.

C.2 Interworking between an EDI-UA and a 1984 UA

This clause specifies the interworking between an implementation of the AMH3 profile and an implementation of an EDI-UA on a 1984 MTS.

It is based on the following principals:

- Downgrading of the MTS is according to the downgrading rules between 1988 and 1984 systems as defined in ISO/IEC 10021-6 and further classified in ISP 10611-1.
- Rules are defined in this clause for Elements of Service which require a 1988 MTS and cannot be downgraded.

An EDI-UA may support downgrading of service elements requested by an EDI Application as specified in Table C.1 and C.2.

Table C.1 - Classification of Downgrading Actions for EDIMG EoS

Element of Service	Action
Incomplete Copy Indication	D
Non Repudiation of Content Originated	R
Non Repudiation of Content Received	R
Non Repudiation of Content Received Request	R
Non Repudiation of Delivery	D
Non Repudiation of EDI Notification	R
Non Repudiation of EDI Notification Request	R
Proof of Content Received	R
Proof of Content Received Request	R
Proof of EDI Notification	R
Proof of EDI Notification Request	R

Table C.2 - Classification of Downgrading Actions MT EoS

Element of Service	Action
Additional Physical Rendition	D
Basic Physical Rendition	D
Content Confidentiality	D
Content Integrity	R
Conversion Prohibition in Case of Loss of Information	D
Counter Collection	D
Counter Collection with Advice	D
Delivery via Bureaufax Service	D
Designation of Recipient by Directory Name	D
DL Expansion History Indication	D
DL Expansion Prohibited	D
EMS (Express Mail Service)	D
Latest Delivery Designation	D
Message Flow Confidentiality	D
Message Origin Authentication	R
Message Security Labelling	D
Message Sequence Integrity	D

Element of Service	Action
Non Repudiation of Origin	D
Non Repudiation of Submission	D
Ordinary Mail	D
Originator Requested Alternate Recipient	D
Physical Delivery Notification by MHS	D
Physical Delivery Notification by PDS	D
Physical Forwarding Allowed	D
Physical Forwarding Prohibited	D
Probe Origin Authentication	D
Proof of Delivery	D
Proof of Submission	D
Redirection Disallowed by Originator	D
Redirection of Incoming Messages	D
Registered Mail	D
Registered Mail to Addressee in Person	D
Report Origin Authentication	D
Request for Forwarding Address	D
Requested Delivery Method	D
Secure Access Management	D
Special Delivery	D
Use of Distribution List	D
User/UA Capabilities Registration	D

Legend tables C.1 and C.2:

D: Corresponding protocol elements or service requests are downgraded. The notification of this action to the EDI Application is a local matter.

R: Attempted use of this service will cause the complete message to be rejected. The EDI application should be notified but the mechanism for this is a local matter.

C.3 Interworking between an EDI-UA and a 1984 MTA

Submission of EDIMs and EDINs to 1984 MTA and delivery of EDIMs and EDINs from a 1984 MTA is specified in ISO/IEC 10021-9 clause 19.

C.4 Interworking between EDIMG systems and IPM systems

This scenario specifies the conversion between systems using the P2 approach for EDI and systems using Pedi. The P2 approach specifies how an EDI Interchange can be carried in an IPM over 1984 MTS. The EDI interchange is carried as an IA5string in the text part of the IPM Content.

C.4.1 Conversion from EDIM to IP-message

The verification of authority to perform a particular conversion is outside the scope of this annex. It is assumed that such conversions will be done with the full knowledge of the originating and recipient parties. Any conversion will at least be ruled by any conversion prohibition or conversion prohibition in case of loss request.

The EDIFACT ISO646 EDI body part of the EDIM is copied to the IPM Body as an IA5 Text body part. All other body parts of the EDIM will be discarded and this action is treated as a conversion. The encode information type (EIT) on the message envelope is IA5Text. The conversion fails if the EDI body part is not an EDIFACT ISO646 body part.

The IPM Heading fields are set as follows:

IPMIdentifier: EDIMIdentifier

Originator: Originator ORName

Recipients: Recipients from the EDIM Heading. All recipients become IPM Primary recipients. The conversion fails if any EDIN is requested. IPM Notifications are not requested.

Subject: Not present, or set to a value according to local policy.

C.4.2 Conversion from IP-message to EDIM

It is assumed that there is one and only one body part in the IPM Message, and that this body part contains an EDI Interchange.

The IPM body part becomes the first, and only, body part of the EDIM.

The EDIM Heading fields are set as follows:

EDIM Identifier: Originator ORName concatenated with the Local IPMIdentifier portion of the IPMIdentifier.

Originator: Originator ORName.

Recipients: Recipient ORNames from the IPM Heading. The edi notification requests field is not coded.

EDIBodyPartType:
The value is a local implementation issue. If the entity performing the conversion can identify the EDI syntax of the EDI Interchange then it can specify an appropriate value. Otherwise, the entity must be assuming a specific encoding and will specify the value for the syntax it is assuming.

Other heading fields may be set if the entity performing the conversion is capable of parsing the EDI Interchange and discovering the correct values of the EDIM Heading fields.

Since there are no notification requests the EDI-UA will never create an EDIN when it receives a converted EDIM and therefore the action for handling EDINs in the reverse direction does not need to be considered.

Annex D

(informative)

AMH3n - overall scope and applicability

D.1 Introduction

This annex provides some general background on the scope and applicability of the AMH3 profiles as specified in this multipart ISP.

D.2 Message Handling profiles

The AMH profiles are applicable to end systems operating in an Open System Interconnection (OSI) environment which forms part of a Message Handling System (MHS) environment based on ISO/IEC 10021 and the equivalent ITU-T X.400 series of Recommendations.

The AMH1n set of profiles covers Common Messaging - i.e. those aspects of the MHS based standards which are independent of a particularly messaging context (content type). Such requirements are considered to be 'generic' and are expected to be supported by all MHS implementations.

Further content type-specific sets of profiles specify additional requirements which are applicable to particular MHS application scenarios as represented by particular classes of user agent (UA) and content protocol.

The content type-specific profile sets cover both end-to-end UA-to-UA communication (the content protocol and associated UA functionality) and use of Messaging Handling services (by requiring conformance to the appropriate AMH1 profile(s) plus support of any additional content type-specific requirements).

D.3 AMH3 profiles

AMH3 set of profiles cover EDI Messaging (EDIMG), which is designed to support electronic data interchange (EDI) between application processes.

The AMH3n profiles each specify a particular combination of OSI standards which collectively provide one of the MHS services as realised by an MHS protocol, as applicable in an EDIMG context:

- AMH31 - EDIMG Content (Pedi protocol) - between EDIMG user agents (UAs);
- AMH32 - EDIMG Requirements for Message Transfer (P1 protocol) - between message transfer agents (MTAs);
- AMH33 - EDIMG Requirements for Message Transfer System (MTS) Access (P3 protocol) - between a remote UA and an MTA, and between a remote message store (MS) and an MTA;
- AMH35 - EDIMG Requirements for Message Transfer System (MTS) Access (P3 protocol) - The "AMH33" for the revised 1995 edition of the base standard;
- AMH34 - EDIMG Requirements for Enhanced Message Store (MS) Access (P7 protocol) - between a remote UA and an MS (the AMH13 profile allows minimal support of EDIMG-specific MS attributes to be claimed; the AMH34 profile requires more extensive support of EDIMG-specific MS attributes). Based on the 1988/1990/1992 base standard.