INTERNATIONAL STANDARDIZED PROFILE

ISO/IEC ISP 12062-1

Third edition
2003-06-15

Information technology — International Standardized Profiles AMH2n — Message Handling Systems — Interpersonal Messaging —

Part 1: IPM MHS Service Support

Technologies de l'information — Profils normalisés internationaux AMH2n — Systèmes de messagerie — Messagerie entre personnes —

Partie 1: Support de service de IPM MHS

IECNORM.COM : Click to view the full PDF of ISO/IEC ISP 12062-1:2003

Reference number
ISO/IEC ISP 12062-1:2003(E)

© ISO/IEC 2003

PDF disclaimer

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

Adobe is a trademark of Adobe Systems Incorporated.

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

IECNORM.COM : Click to view the full PDF of ISO/IEC ISP 12062-1:2003

© ISO/IEC 2003

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

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

 © ISO 2003 — All rights reserved

Contents

IECNORM.COM : Click to view the full PDF of ISO/IEC ISP 12062-1:2003

© ISO 2003 — All rights reserved

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 shall not be held responsible for identifying any or all such patent rights.

ISO ISP 12062-1 was prepared by Technical Committee ISO/TC 1, *Information technology*, Subcommittee SC 6, *Telecommunications and information exchange between systems*.

This third edition cancels and replaces the second edition (ISO/IEC ISP 12062-1:1998), which has been technically revised.

ISO/ISP 12062 consists of the following parts, under the general title *Information technology — International Standardized Profiles AMH2n — Message Handling Systems — Interpersonal Messaging*:

— *Part 1: IPM MHS Service Support*

— *Part 2: AMH21 — IPM Content*

— *Part 3: AMH22 — IPM Requirements for Message Transfer (P1)*

— *Part 4: AMH23 and AMH25 — IPM Requirements for MTS Access (P3) and MTS 94 Access (P3)*

— *Part 5: AMH24 — IPM Requirements for Enhanced MS Access (P7)*

— *Part 6: AMH26 — IPM Requirements for Enhanced MS 94 Access (P7)*

IECNORM.COM : Click to view the full PDF of ISO/IEC ISP 12062-1:2003

© ISO 2003 — All rights reserved

Introduction

This part of ISO/IEC ISP 12062 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 12062 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 12062 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 12062 will remain available for an overlap period.

IECNORM.COM : Click to view the full PDF of ISO/IEC ISP 12062-1:2003

© ISO 2003 — All rights reserved

Information technology — International Standardized Profiles AMH2n — Message Handling Systems — Interpersonal Messaging —

Part 1: IPM MHS Service Support

IECNORM.COM : Click to view the full PDF of ISO/IEC ISP 12062-1:2003

1 Scope

1.1 General

This part of ISO/IEC ISP 12062 contains the overall specifications of the support of MHS Elements of Service and associated MHS functionality in an Interpersonal Messaging (IPM) environment which are generally not appropriate for consideration only from the perspective of a single MHS protocol. These specifications form part of the Interpersonal Messaging application functions, as defined in the parts of ISO/IEC ISP 12062, 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 Interpersonal Messaging application profiles ISO/IEC ISP 12062-2 (AMH21), ISO/IEC ISP 12062-3 (AMH22), ISO/IEC ISP 12062-4 (AMH23 and AMH25), ISO/IEC ISP 12062-5 (AMH24) and ISO/IEC ISP 12062-6 (AMH26), which specify the support of specific MHS protocols and associated functionality.

The specifications in this part of ISO/IEC ISP 12062 are divided into **basic requirements**, which are required to be supported by all IPM MHS 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 AMH2n 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 12062 is the first part, as common text, of a multipart ISP identified in ISO/IEC TR 10000-2 as “AMH2, Message Handling Systems - Interpersonal Messaging” (see also ISO/IEC TR 10000-1, 8.2 for the definition of multipart ISPs).

This part of ISO/IEC ISP 12062 does not, on its own, specify any profiles.

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.

© ISO 2003 — All rights reserved

NOTES

1 - References in the body of this part of ISO/IEC ISP 12062 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 E.

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.413 (1999) | ISO/IEC 10021-5: 1999, *Information technology - Message Handling Systems (MHS): Message store: Abstract service definition*

ITU-T Recommendation X.420 (1999) | ISO/IEC 10021-7:—[3)], *Information technology - Message Handling Systems (MHS) - Interpersonal messaging system*

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

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 12062 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 12062).

---

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

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

3) To be published. (Revision of ISO/IEC 10021-7:1997)

IECNORM.COM : Click to view the full PDF of ISO/IEC ISP 12062-1:2003

© ISO 2003 — All rights reserved

3.2 Support classification

To specify the support level of Elements of Service for this part of ISO/IEC ISP 12062, the following terminology is defined.

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 rôle of originator; a service user (i.e. a UA) shall be able to use the Element of Service in the rôle of originator.

for IPM Elements of Service:

a service provider (i.e. an IPM UA) shall implement all 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 rôle 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. an MTA or MS) shall be able to make the Element of Service available to a service user in the rôle of recipient; a service user (i.e. a UA) shall be able to use the Element of Service in the rôle of recipient.

for IPM Elements of Service:

a service provider (i.e. an IPM UA) shall implement all 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 rôle 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.

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.

conditional support (**c**) : the Element of Service shall be supported under the conditions specified in this part of ISO/IEC ISP 12062. 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).

out of scope (**i**) : the Element of Service is outside the scope of this part of ISO/IEC ISP 12062 - 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 this ISP.

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

IECNORM.COM : Click to view the full PDF of ISO/IEC ISP 12062-1:2003

© ISO 2003 — All rights reserved

3.3 Profile object identifiers

Profiles that are specified in ISO/IEC ISP 12062 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 this ISP.

Table 1 - Profile object identifiers

Profile	Object Identifier
AMH21	{ iso(1) standard(0) interpersonal-messaging(12062) ipm-content(2) }
AMH22	{ iso(1) standard(0) interpersonal-messaging(12062) ipm-message-transfer(3) }
AMH23	{ iso(1) standard(0) interpersonal-messaging(12062) ipm-mts-access(4) }
AMH24	{ iso(1) standard(0) interpersonal-messaging(12062) ipm-ms-access(5) }
AMH25	{ iso(1) standard(0) interpersonal-messaging(12062) ipm-mts-94-access(6) }
AMH26	{ iso(1) standard(0) interpersonal-messaging(12062) ipm-ms-94-access(7) }

IECNORM.COM : Click to view the full PDF of ISO/IEC ISP 12062-1:2003

4 Abbreviations

84IW	84 Interworking
AA	Auto-Annotation
AACK	Auto-Acknowledgement
AADV	Auto-Advise
AC	Auto-Correlation
AD	Auto-Deletion
ADIS	Auto-Discard
AF	Auto-Forward
AG	Auto-Grouping
AMH	Application Message Handling
ALERT	Alert
ASN.1	Abstract Syntax Notation One
BC	Business Class
CV	Conversion
DC	Delivery Constraints
DIR	Use of Directory
DL	Distribution List
EoS	Element of Service
FG	Functional group
FWD	Manual Forwarding
IPM	Interpersonal Messaging
ISP	International Standardized Profile
LD	Latest Delivery
LOG	Logging
MHS	Message Handling Systems
MS	Message store
MT	Message transfer
MTA	Message transfer agent
MTS	Message Transfer System
ORAM	OR-address Matching
ORNM	OR-name Matching
OSI	Open Systems Interconnection
PD	Physical Delivery
PDAU	Physical delivery access unit
RED	Redirection
RED2	Redirection Instructions
RD	Restricted Delivery
RoC	Return of Content

© ISO 2003 — All rights reserved

SDM	Storage of Draft Messages
SEC	Security
SG	Storage and Grouping
SMI	Stored Message Incorporation
SPP	Simple Protected Password
STAT	Action Status
TRASH	Trash
UA	User agent

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 12062.

NOTE - This part of ISO/IEC ISP 12062 is a reference specification of the basic requirements and functional groups covered by the AMH2n set of profiles and is additional to the protocol-specific requirements specified in the following parts of ISO/IEC ISP 12062. Although this part of ISO/IEC ISP 12062 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 12062 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 programmatic interface) may be provided, but are not required for conformance to this version of ISO/IEC ISP 12062.

6 Basic requirements

Annex A specifies the basic requirements for support of MHS Elements of Service (EoS) for conformance to ISO/IEC ISP 12062. Basic requirements specify the level of support required by all IPM MHS implementations, as appropriate 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 12062 shall conform to the basic requirements of ISO/IEC ISP 10611, as appropriate to the type of MHS functional object.

6.1 Message length

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

6.2 Number of recipients

If a UA implementation imposes any limit on the number of recipients that can be specified in an IPM heading, then such limit shall be stated in the PICS.

IECNORM.COM : Click to view the full PDF of ISO/IEC ISP 12062-1:2003

© ISO 2003 — All rights reserved

7 Functional groups

Annex A also 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 subclauses summarize the functionality supported by each of the optional FGs and identify any particular requirements or implementation considerations which are outside the scope of formal conformance to ISO/IEC ISP 12062. 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 and 3. Table 3 lists the functional groups which are only applicable when claiming conformance to AMH26.

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 this ISP, according to the protocol(s) to which each functional group relates.

Table 2 - Summary of AMH2n optional functional groups

Functional Group	Inheritance from AMH1n	relevant to a MTA	relevant to a MS	relevant to a UA
IPM Conversion (CV)	inherited [2]	Y	N	Y
IPM Distribution List (DL)	inherited [2]	Y	Y[3]	Y[3]
IPM Physical Delivery (PD)	inherited [1]	Y	N	Y
IPM Manual Forwarding (FWD)	new	N	N	Y
IPM Redirection (RED)	inherited [1]	Y	N	Y
IPM Latest Delivery (LD)	inherited [1]	Y	N	Y
IPM Return of Content (RoC)	inherited [1]	Y	Y	Y
IPM Security (SEC0, SEC1, SEC2, SEC2R, SECIW) (SEC0C) (S0) (S0C, S1, S1C, S2, S2C)	 new new inherited [1] inherited [2]	 N Y N Y	 Y Y Y Y	 Y Y Y Y
IPM Use of Directory (DIR)	inherited	Y	Y[4]	Y
IPM 84 Interworking (84IW)	inherited	Y	N	Y
IPM Simple Protected Password (SPP)	inherited [1]	Y	Y	Y
IPM Redirection Instructions (RED2)	inherited [1]	Y	N	Y
IPM Delivery Constraints (DC)	inherited [1]	Y	N	Y
IPM Restricted Delivery (RD)	inherited [1]	Y	N	Y
IPM Business Class (BC)	new	N	Y	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.
3 Only the DL+ER class applies to an MS or to a UA.
4 Only the DIR+SEC class applies to an MS.

IECNORM.COM : Click to view the full PDF of ISO/IEC ISP 12062-1:2003

© ISO 2003 — All rights reserved

Table 3 - Summary of AMH26 optional functional groups

Functional Group	Inheritance from AMH1n	relevant to a MTA	relevant to a MS	relevant to a UA
IPM Storage and Grouping (SG)	inherited	N	Y	Y
IPM Alert (ALERT)	inherited [1]	N	Y	Y
IPM Auto-Annotation (AA)	inherited [1]	N	Y	Y
IPM Auto-Grouping (AG)	inherited [1]	N	Y	Y
IPM Trash (TRASH)	inherited [1]	N	Y	Y
IPM Auto-Deletion (AD)	inherited [1]	N	Y	Y
IPM Auto-Correlation (AC)	inherited [1]	N	Y	Y
IPM Logging (LOG)	inherited [1]	N	Y	Y
IPM Storage of Draft Messages (SDM)	inherited	N	Y	Y
IPM ORAddress Matching (ORAM)	inherited	N	Y	Y
IPM ORName Matching (ORNM)	inherited	N	Y	Y
IPM Auto-Discard (ADIS)	new	N	Y	Y
IPM Auto-Forwarding (AF)	new	N	Y	Y
IPM Auto-Acknowledgement (AACK)	new	N	Y	Y
IPM Auto-Advise (AADV)	new	N	Y	Y
IPM Action Status (STAT)	new	N	Y	Y
IPM Stored Message Incorporation (SMI)	new	N	Y	Y
1 There are no additional requirements to those specified in ISO/IEC ISP 10611.				

IECNORM.COM : Click to view the full PDF of ISO/IEC ISP 12062-1:2003

7.1 IPM Conversion (CV)

The IPM Conversion FG covers support of those EoS which provide the functionality required to perform the action of message body part conversion. Support of the IPM CV FG is applicable to an MTA or a UA. Support of the IPM CV FG by an MTA covers support of either or both of the Explicit Conversion and Implicit Conversion EoS. Support of the IPM CV FG by a UA covers support of the Explicit Conversion EoS only.

NOTE - Support of EoS associated with conversion prohibition is a basic MTA requirement, but this does not imply a capability to perform conversion.

A UA implementation conforming to the IPM CV FG shall support use of the MT Explicit Conversion EoS and the MT Conversion Prohibition in Case of Loss of Information EoS. It shall be stated in the PICS which encoded information type conversions the UA can request.

© ISO 2003 — All rights reserved

An MTA implementation conforming to the IPM CV FG shall conform to the Common Messaging CV FG as specified in ISO/IEC ISP 10611 in an IPM context (i.e. the ability to perform conversion of IPM body parts is required).

7.2 IPM Distribution List (DL)

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

An implementation conforming to the IPM DL FG shall conform to the Common Messaging DL FG as specified in ISO/IEC ISP 10611.

7.3 IPM Physical Delivery (PD)

The IPM Physical Delivery FG is concerned with access to physical delivery (i.e. postal, courier, etc) services. The IPM 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 is applicable to an MTA or a UA. Support of a PDAU is only applicable to an MTA. The requirements for the PDAU itself are outside the scope of this ISP.

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

7.4 IPM Manual Forwarding (FWD)

The IPM Manual Forwarding FG covers support for forwarding of messages by the MHS user. Support of the IPM FWD FG is only applicable to a UA.

A UA implementation conforming to the IPM FWD FG shall support the Forwarded IP-message Indication EoS on origination.

7.5 IPM Redirection (RED)

The IPM 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. Support of the IPM RED FG is applicable to an MTA or a UA.

An MTA implementation conforming to the IPM 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 IPM environment.

A UA implementation conforming to the IPM RED FG shall support use of the following MT EoS:

- Alternate Recipient Allowed
- Originator Requested Alternate Recipient
- Redirection of Incoming Messages

7.6 IPM Latest Delivery (LD)

The IPM 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. Support of the IPM LD FG is applicable to an MTA or a UA.

An implementation conforming to the IPM 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 UA in an IPM environment.

IECNORM.COM : Click to view the full PDF of ISO/IEC ISP 12062-1:2003

© ISO 2003 — All rights reserved

7.7 IPM Return of Content (RoC)

The IPM Return of Content FG covers support of the Return of Content EoS - i.e. the functionality required to cause the contents of a submitted message to be returned in any non-delivery notification if so requested by the originator. Support of the IPM RoC FG is applicable to an MTA, an MS or a UA.

NOTE - The IPM RoC FG is concerned only with the return of content in a non-delivery notification, not with return of an IPM in a non-receipt notification.

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

7.8 IPM Security (SEC0, SEC0C, SEC1, SEC2, SEC2R, SECIW, S0, S0C, S1, S1C, S2, S2C)

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

The IPM Security FG is specified as six largely independent **security classes** denoted as SEC0, SEC0C, SEC1, SEC2, SEC2R and SECIW. In addition to these, an IPM implementation can support any of the Common Messaging security classes S0, S0C, S1, S1C, S2 and S2C.

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

The security classes SEC2 and SEC2R require support of the Content Integrity EoS. SEC2R 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 7.8.2.).

7.8.1 IPM specific security classes (SEC0, SEC0C, SEC1, SEC2, SEC2R, SECIW)

The IPM Security FG supports use of IPM security services and functionality as follows :

IECNORM.COM : Click to view the full PDF of ISO/IEC ISP 12062-1:2003

© ISO 2003 — All rights reserved

Table 4 - IPM Security Classes

Element of Service	Security Class					
	SEC0	SEC0C	SEC1	SEC2	SEC2R	SECIW
Body Part Authentication and Integrity	m	m	c [1]	–	–	–
Body Part Encryption	o	m	o	–	–	m
Content Integrity	–	–	c [1]	m	m	–
IP-message Security Labelling	o	o	m	–	–	–
Message Origin Authentication	–	–	c [1]	o	m	
Non-repudiation of Content Received	–	–	–	o	m	–
Request for Non-repudiation of Content Received	–	–	–	o	m	–
Non-repudiation of IP-notification	–	–	–	o	m	–
Request for Non-repudiation of IP-notification	–	–	–	o	m	–
Proof of Content Received	–	–	–	m	m	–
Request for Proof of Content Received	–	–	–	m	m	–
Proof of IP-notification	–	–	–	m	m	–
Request for Proof of IP-notification	–	–	–	m	m	–

1 Either the Body Part Authentication and Integrity, or the Content Integrity, or the Message Origin Authentication security service is mandatory.

IECNORM.COM : Click to view the full PDF of ISO/IEC ISP 12062-1:2003

Security class SEC0 requires that security measures shall be provided by the IPM system implementation in order to provide authentication and integrity of individual body parts. It provides similar functionality to S0, but applied to individual body parts instead of to the entire content.

Security class SEC0C requires that security measures shall be provided by the IPM system implementation in order to provide authentication, integrity and confidentiality of individual body parts. It adds body part confidentiality to SEC0, and thus provides similar functionality to S0C, but applied to individual body parts instead of to the entire content.

Security class SEC1 requires that security measures shall be provided by the IPM system implementation in order to provide authentication, integrity and security labelling of individual body parts. It adds body part security labelling to SEC0, and thus provides similar functionality to S1, but applied to individual body parts instead of to the entire content.

Security class SEC2 requires that security measures shall be provided by the IPM system implementation in order to provide UA to UA proof services for messages and notifications. It is independent of all classes other than SEC2R, and can be combined with any other IPM or Common Messaging security classes.

Security class SEC2R requires that security measures shall be provided by the IPM system implementation in order to provide UA to UA non-repudiation services for messages and notifications. It adds non-repudiation properties to the services in SEC2, but is independent of all other classes and can be combined with any other IPM or Common Messaging security classes.

© ISO 2003 — All rights reserved

Security class SECIW requires that security measures shall be provided by the IPM system implementation in order to provide authentication, integrity and confidentiality in a body part encoded in a messaging-system independent format. It is intended to allow secure interworking with messaging systems implementing other protocols, and as this is the only class providing security services independent of the supporting messaging protocol it will not usually be useful to combine this class with any other security class. This class provides similar services to SEC0C but the alternative protocol encoding prevents some functionality, such as forwarding or Distribution List expansion of messages with confidentiality services.

7.8.2 Common messaging Security (Sn, SnC)

The Common messaging Security classes covers the provision of secure messaging in an IPM 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 as specified in ISO/IEC ISP 10611. There are no additional requirements for an MTA, UA or MS in an IPM environment.

7.9 IPM Use of Directory (DIR)

The IPM Use of Directory functional group 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).

NOTE - 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 this ISP.

An implementation conforming to the IPM 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 in an IPM environment.

7.10 IPM 84 Interworking (84IW)

The 84 Interworking functional group covers interworking between implementations conforming to ISO/IEC ISP 12062 (hereafter referred to as '1988 systems') and implementations conforming to the CCITT X.400(1984) Recommendations (hereafter referred to as '1984 systems').

IECNORM.COM : Click to view the full PDF of ISO/IEC ISP 12062-1:2003

© ISO 2003 — All rights reserved

Support of the 84IW FG is applicable to an MTA or a UA.

An MTA implementation conforming to the IPM 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 IPM environment.

A UA implementation conforming to the IPM 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 of IA5 Text body parts.

Additional recommended practices for interworking with 1984 systems are described in annex C, covering procedures for downgrading IPM content type 22 to content type 2.

7.11. IPM Simple Protected Password (SPP)

The IPM 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 1996-1997 publication of the MHS base standards.

An implementation conforming to the IPM Simple Protected Password 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 IPM environment.

7.12. IPM Redirection instructions (RED2)

The IPM 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 IPM 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 IPM environment.

7.13. IPM Delivery constraints (DC)

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

An implementation conforming to the IPM 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 IPM environment.

7.14. IPM Restricted Delivery (RD)

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

An implementation conforming to the IPM 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 IPM environment.

7.15. IPM Business Class (BC)

This Functional Group encompasses the functionality provided by the following Elements of Service, as defined in ISO/IEC 10021-1.

- Authorization Time Indication
- Circulation List Recipients Indication
- Distribution Codes Indication

IECNORM.COM : Click to view the full PDF of ISO/IEC ISP 12062-1:2003

© ISO 2003 — All rights reserved

- Information Category Indication
- Manual Handling Instructions Indication
- Originator Reference Indication
- Precedence Indication

7.16. IPM Storage and Grouping (SG)

This Functional Group encompasses the functionality to attach group-names to messages stored in the MS, provided by the following Elements of Service, as defined in ISO/IEC 10021-1.

- Storage on Submission
- Stored Message Grouping

7.17. IPM Alert (ALERT)

This Functional group encompasses the functionality for a UA to request and to be informed of the arrival of selected new messages, as provided by the Element of Service Stored Message Alert, as defined in ISO/IEC 10021-1.

7.18. IPM Auto-Annotation (AA)

This Functional Group encompasses the functionality to attach information which is only available to the user, as provided by the following Elements of Service, as defined in ISO/IEC 10021-1.

- Stored Message Annotation
- Auto-assignment of Annotations
- Auto-action Log

7.19. IPM Auto-Grouping (AG)

This Functional Group encompasses the functionality to attach group-names to messages stored in the MS, provided by the following Elements of Service, as defined in ISO/IEC 10021-1.

- Stored Message Grouping
- Auto-assignment of Group Names
- Auto-action Log

7.20. IPM Trash (TRASH)

This Functional Group covers those aspects which enable the user to manually delete messages he has previously explicitly marked for deletion. To achieve this functionality, the MS and UA must support the Modify operation and the attribute Marked-for-deletion.

7.21. IPM Auto-Deletion (AD)

This Functional Group encompasses the functionality to assign automatically a period after which messages meeting the specified selection criteria will be deleted from the MS, as provided by the following Elements of Service, as defined in ISO/IEC 10021-1.

- Storage Period Assignment

IECNORM.COM : Click to view the full PDF of ISO/IEC ISP 12062-1:2003

© ISO 2003 — All rights reserved

- Auto-deletion after Storage Period
- Auto-action Log
- Auto-assignment of Storage Period

7.22. IPM Auto-Correlation (AC)

This Functional Group encompasses functionality related to auto-correlation of reports, IP-notifications and IP-messages. It is specified as three incremental classes AC0, AC1 and AC2.

AC0 This IPM auto-correlation class encompasses the functionality provided by the following Elements of Service, as defined in ISO/IEC 10021-1.

- Storage on Submission
- Auto-correlation of Reports
- Auto-correlation of IP-notifications

AC1 This IPM auto-correlation class encompasses the functionality provided in AC0 and, in addition, the functionality linked to the auto-correlation of replies which forms part of the following Element of Service, defined in ISO/IEC 10021-1.

- Auto-correlation of IP-messages

AC2 This IPM auto-correlation class encompasses the functionality provided in AC0 and, in addition, all the functionality provided by the following Element of Service, defined in ISO/IEC 10021-1.

- Auto-correlation of IP-messages

7.23. IPM OR-address Matching (ORAM)

This Functional Group provides the capability to select entries in the MS by specifying a filter in which properties of an OR-address are specified. In an IPM environment, this FG includes matching an OR-address within IPM fields (e.g. within OR-descriptor, or within recipient-specifier).

7.24. IPM OR-name Matching (ORNM)

This Functional Group provides the capability to select entries in the MS by specifying a filter in which properties of an OR-name are specified. In an IPM environment, this FG includes matching an OR-name within IPM fields (e.g. within OR-descriptor, or within recipient-specifier).

7.25. IPM Storage of Draft Messages (SDM)

This Functional Group encompasses the functionality for a UA to store draft messages in a MS, as provided by the Element of Service Storage of Draft Messages, as defined in ISO/IEC 10021-1.

7.26. IPM Logging (LOG)

This Functional Group encompasses the functionality provided by the following Elements of Service, as defined in ISO/IEC 10021-1.

- Delivery Log
- Submission Log

IECNORM.COM : Click to view the full PDF of ISO/IEC ISP 12062-1:2003

© ISO 2003 — All rights reserved

7.27. IPM Auto-Discard (ADIS)

This Functional Group encompasses the functionality provided by the following Elements of Service, as defined in ISO/IEC 10021-1.

- Auto-discarding of IP-messages
- Auto-action Log

7.28. IPM Auto-Forward (AF)

This Functional Group encompasses the functionality provided by the following Elements of Service, as defined in ISO/IEC 10021-1.

- Auto-forwarding of IP-messages
- Auto-action Log

7.29. IPM Auto-Acknowledgement (AACK)

This Functional Group encompasses the functionality provided by the following Elements of Service, as defined in ISO/IEC 10021-1.

- Auto-acknowledgement of IP-messages
- Auto-action Log

7.30. IPM Auto-Advise (AADV)

This Functional Group encompasses the functionality provided by the following Elements of Service, as defined in ISO/IEC 10021-1.

- IPM Auto-advise
- Auto-action Log

7.31. IPM Action Status (STAT)

This Functional Group encompasses the functionality provided by the following Element of Service, as defined in ISO/IEC 10021-1.

- IP-message Action Status

7.32. IPM Stored Message Incorporation (SMI)

This Functional Group encompasses the functionality provided by the following Element of Service, as defined in ISO/IEC 10021-1.

- Submission of IP-messages Incorporating Stored Messages

8 Naming and addressing

Implementations shall support naming and addressing capabilities as specified in clause 8 of ISO/IEC ISP 10611-1. In addition, a UA implementation shall support use of the numeric and terminal OR-address forms to identify recipients (support of these forms to identify the UA itself is not required).

IECNORM.COM : Click to view the full PDF of ISO/IEC ISP 12062-1:2003

© ISO 2003 — All rights reserved

9 Error and exception handling

The upper bounds defined in annex L of ISO/IEC 10021-7 are normative for the purposes of this ISP.

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.

IECNORM.COM : Click to view the full PDF of ISO/IEC ISP 12062-1:2003

© ISO 2003 — All rights reserved

Annex A

(normative)

Elements of Service

In the event of a discrepancy becoming apparent in the body of this part of ISO/IEC ISP 12062 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 IPM environment (i.e. IPM UA) for conformance to ISO/IEC ISP 12062. Whether such services are made available to the MHS user is covered in the AMH21 PICS proforma.

In the following tables, the "Basic" column reflects the basic requirements for conformance to ISO/IEC ISP 12062 - i.e. the minimum level of support required by all IPM 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 IPM 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			

IECNORM.COM : Click to view the full PDF of ISO/IEC ISP 12062-1:2003

© ISO 2003 — All rights reserved

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

Element of Service	Basic		Functional Group		
	Orig.	Rec.	FG	Orig.	Rec.
Additional Physical Rendition	o	–			
Alternate Recipient Allowed	o	–	RED	m	
Alternate Recipient Assignment[2]	–	–			
Basic Physical Rendition	o	–	PD	m	
Content Confidentiality	o	o	SEC	c[1]	c[1]
Content Integrity	o	o	SEC	c[1]	c[1]
Conversion Prohibition	m	m			
Conversion Prohibition in Case of Loss of Information	o	o	CV	m	m
Counter Collection	o	–	PD	m	
Counter Collection with Advice	o	–			
Cover Page Suppression	o	o			
Deferred Delivery	m	–			
Deferred Delivery Cancellation[3]	m	–			
Delivery Notification	m	–			
Delivery via Bureaufax Service	o	–			
Designation of Recipient by Directory Name	o	–	DIR	m	
Disclosure of Other Recipients	o	m			
DL Exempted Recipients	o	o	DL+ER	m	m
DL Expansion History Indication	–	m			
DL Expansion Prohibited	m[4]	–			
EMS (Express Mail Service)	o	–	PD	m	
Explicit Conversion	o	–	CV	m	
Grade of Delivery Selection	m	m			
Hold for Delivery	–	o			
Implicit Conversion	–	–			
Latest Delivery Designation	o	–	LD	m	

IECNORM.COM : Click to view the full PDF of ISO/IEC ISP 12062-1:2003

© ISO 2003 — All rights reserved

Element of Service	Basic		Functional Group		
	Orig.	Rec.	FG	Orig.	Rec.
Message Flow Confidentiality	i	i			
Message Origin Authentication	o	o	SEC	c[1]	c[1]
Message Security Labelling	o	o	SEC	c[1]	c[1]
Message Sequence Integrity	o	o			
Multi-destination Delivery	m	–			
Non-repudiation of Delivery	o	o	SEC	c[1]	c[1]
Non-repudiation of Origin	o	o	SEC	c[1]	c[1]
Non-repudiation of Submission	i	–	SEC	c[1]	
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	–	SEC	c[1]	
Proof of Delivery	o	o	SEC	c[1]	c[1]
Proof of Submission	i	–	SEC	c[1]	
Redirection Disallowed by Originator	m[4]	–			
Redirection of Incoming Messages [5]	–	o	RED		m
Registered Mail	o	–			
Registered Mail to Addressee in Person	o	–			
Report Origin Authentication	i	i	SEC	c[1]	c[1]
Request for Forwarding Address	o	–			
Requested Preferred Delivery Method	o	–			

IECNORM.COM : Click to view the full PDF of ISO/IEC ISP 12062-1:2003

© ISO 2003 — All rights reserved

Element of Service	Basic		Functional Group		
	Orig.	Rec.	FG	Orig.	Rec.
Restricted Delivery	–	i			
Return of Content	o	–	RoC	m	
Secure Access Management	o	o	SEC	c[1]	c[1]
Special Delivery	o	–	PD	m	
Undeliverable Mail with Return of Physical Message	o	–	PD	m	
Use of Distribution List	m[6]	–			

NOTES

1 Support is according to the security class for which support is claimed - see clause A.1 of ISO/IEC ISP 10611-1.

2 The method by which an alternate recipient is specified to the MTA is outside the scope of this ISP.

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

4 Support of this EoS has been made mandatory as the default is "allowed" (the capability to generate both the "prohibited" value and the "allowed" value is required).

5 It is not required that 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

This clause specifies the requirements for a MS or MS-user component that implements MS Elements of Service as defined in the 19902 publication of the base standard, and which therefore claims conformance to AMH25 (and AMH13).

The requirements for support of MS EoS by an MS are as specified in clause A.2 of ISO/IEC ISP 10611-1. The following tables specify the requirements for use of such services by an MS-user in an IPM environment (i.e. IPM UA) for conformance to ISO/IEC ISP 12062. Whether such services are made available to the MHS user is covered in the AMH21 PICS proforma.

In the following tables, the "Basic" column reflects the basic requirements for conformance to ISO/IEC ISP 12062 - i.e. the minimum level of support required by all IPM 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 Message Store

Element of Service	Basic	Functional Group	
	MS-user	FG	UA
MS Register	o		
Stored Message Deletion	m		

IECNORM.COM : Click to view the full PDF of ISO/IEC ISP 12062-1:2003

© ISO 2003 — All rights reserved

Element of Service	Basic	Functional Group	
	MS-user	FG	UA
Stored Message Fetching	m		
Stored Message Listing	m		
Stored Message Summary	m		

Table A.4 - MS Optional User Facilities

Element of Service	Basic	Functional Group	
	MS-user	FG	UA
Stored Message Alert	o		
Stored Message Auto-forward	o		

A.3 MS94 Elements of Service

The following tables specify the requirements for a MS or MS-user component that implements MS Elements of Service as defined in the 1994-1997 publication of the base standard, which defines several new Elements of Service in addition to those that were defined in the 1990 publication of the base standard. This clause therefore applies to components claiming conformance to AMH26 (and AMH15).

In the following tables, the "Basic" column reflects the basic requirements for conformance to ISO/IEC ISP 12062 - i.e. the minimum level of support required by all IPM-UA and IPM-MS 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"). Each column is further subdivided to distinguish the support required for an MS from that for an MS-user (the latter refers only to the use of MS services, not whether such services are made available to the MHS user, which is covered in the AMH21 PICS proforma).

Table A.5 - Base Message Store 94

Element of Service	Basic		Functional Group		
	MS-user	MS	FG	MS-user	MS
MS Register	o	m			
Stored Message Deletion	m	m			
Stored Message Fetching	m	m			
Stored Message Listing	m	m			
Stored Message Summary	m	m			

IECNORM.COM : Click to view the full PDF of ISO/IEC ISP 12062-1:2003

© ISO 2003 — All rights reserved

Table A.6 - MS Optional User Facilities 94

Element of Service	Basic		Functional Group		
	MS-user	MS	FG	MS-user	MS
Auto-acknowledgement of IP-messages	o	o	AACK	m	m
Auto-action Log	c[1]	c[1]	AA AG AD ADIS AF AACK AADV	m m m m m m m	m m m m m m m
Auto-advise	o	o	AADV	m	m
Auto-assignment of Annotations	o	o	AA	m	m
Auto-assignment of Group Names	o	o	AG	m	m
Auto-assignment of Storage Period	o	o	AD	m	m
Auto-correlation of IP-messages	o	o	AC1,2	m	m
Auto-correlation of IP-notifications	o	o	AC0,1,2	m	m
Auto-correlation of Reports	o	o	AC0,1,2	m	m
Auto-deletion after Storage Period	o	o	AD	m	m
Auto-discarding of IP-messages	o	o	ADIS	m	m
Auto-forwarding of IP-messages	o	o	AF	m	m
Delivery Log	o	o	LOG	m	m
IP-message Action Status	o	o	STAT	m	m
Storage of Draft Messages	o	o	SDM	m	m
Storage on Submission	c[5]	c[5]	SG AC0,1,2	m m	m m
Storage Period Assignment	c[4]	c[4]	AD	m	m
Stored Message Alert	o	o	ALERT	m	m
Stored Message Annotation	c[2]	c[2]	AA	m	m
Stored Message Grouping	c[3]	c[3]	SG AG	m m	m m
Submission Log	c[5]	c[5]	LOG	m	m
Submission of IP-messages Incorporating Stored Messages	o	o	SMI	m	m

IECNORM.COM : Click to view the full PDF of ISO/IEC ISP 12062-1:2003

© ISO 2003 — All rights reserved

NOTES

1 shall be supported if at least one auto-action type is supported

2 this EoS is mandatory if Auto-assignment of Annotations is supported

3 this EoS is mandatory if Auto-assignment of Group Names is supported

4 this EoS is mandatory if at least one of Auto-assignment of Storage Period or Auto-deletion after Storage Period is supported

5 support of at least one of these two EoS's is mandatory if Auto-correlation of Reports, Auto-correlation of IP-notifications or IP-message Action Status is supported

A.4 IPM-specific Elements of Service

The following tables specify the requirements for support of IPM-specific Elements of Service by an MTS-user in an IPM environment (i.e. IPM UA) for conformance to ISO/IEC ISP 12062. Whether such services are made available to the MHS user is covered in the AMH21 PICS proforma.

In the following tables, the "Basic" column reflects the basic requirements for conformance to ISO/IEC ISP 12062 - i.e. the minimum level of support required by all IPM 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.7 - Elements of Service Belonging to The Basic IPM Service (IPM EoS)

Element of Service	Basic		Functional Group		
	Orig.	Rec.	FG	Orig.	Rec.
IP-message Identification	m	m			
Typed Body	m	m			

Table A.8 - IPM Optional User Facilities (IPM EoS)

Element of Service	Basic		Functional Group		
	Orig.	Rec.	FG	Orig.	Rec.
Authorization Time indication	o	o	BC	m	m
Authorizing Users Indication	o	m			
Auto-forwarded Indication	o	m			
Auto-submitted Indication	o	o			
Blind Copy Recipient Indication	o	m			
Body Part Authentication and Integrity	o	o	SEC0, 0C	m	m
Body Part Encryption	o	m	SEC0C	m	m
Circulation List Recipients Indication	o	m	BC	m	m

IECNORM.COM : Click to view the full PDF of ISO/IEC ISP 12062-1:2003

© ISO 2003 — All rights reserved

Element of Service	Basic		Functional Group		
	Orig.	Rec.	FG	Orig.	Rec.
Cross-referencing Indication	o	m			
Distribution Codes Indication	o	o	BC	m	m
Expiry Date Indication	o	m			
Forwarded IP-message Indication	o	m	FWD	m	
Importance Indication	o	m			
Incomplete Copy Indication	o	m			
Information category Indication	o	o	BC	m	m
IP-message Security Labelling	o	o	SEC1	m	m
Language Indication	o	m			
Manual Handling Instructions Indication	o	o	BC	m	m
Multi-part Body	m	m			
Non-receipt Notification Request Indication	o	m[1]			
Non-repudiation of Content Received	o	o	SEC2R	m	m
Non-repudiation of IP-notification	o	o	SEC2R	m	m
Obsoleting Indication	o	m			
Originator Indication	m	m			
Originator Reference Indication	o	o	BC	m	m
Precedence Indication	o	o	BC	m	m
Primary and Copy Recipients Indication	m	m			
Proof of Content Received	o	o	SEC2, 2R	m	m
Proof of IP-notification	o	o	SEC2, 2R	m	m
Receipt Notification Request Indication	o	o	SEC2, 2R	m	m
Reply Request Indication	o	m			
Replying IP-message Indication	m	m			
Request for Non-repudiation of Content Received	o	o	SEC2R	m	m
Request for Non-repudiation of IP-notification	o	o	SEC2R	m	m

IECNORM.COM : Click to view the full PDF of ISO/IEC ISP 12062-1:2003

© ISO 2003 — All rights reserved

Element of Service	Basic		Functional Group		
	Orig.	Rec.	FG	Orig.	Rec.
Request for Proof of Content Received	o	o	SEC2, 2R	m	m
Request for Proof of IP-notification	o	o	SEC2, 2R	m	m
Sensitivity Indication	o	m			
Subject Indication	m	m			

NOTES

1 The capability to generate a non-receipt notification does not have to be demonstrated for an implementation in which a non-receipt condition cannot occur.

IECNORM.COM : Click to view the full PDF of ISO/IEC ISP 12062-1:2003

© ISO 2003 — All rights reserved

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 12062.

None currently, as all approved amendments and corrigenda to ISO/IEC 10021 will be incorporated into the latest edition.

IECNORM.COM : Click to view the full PDF of ISO/IEC ISP 12062-1:2003

© ISO 2003 — All rights reserved

Annex C

(informative)

Additional recommended practices for 1984 interworking

C.1 Introduction

This annex provides some additional recommendations concerning interworking between IPM UA implementations conforming to ISO/IEC ISP 12062 (hereafter referred to as '1988 systems') and IPM UA implementations conforming to earlier versions of the MHS base standards (hereafter referred to as '1984 systems').

Such recommendations are additional to the requirements of the IPM 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 this ISP) 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 interpersonal messages (IPMs) and interpersonal notifications (IPNs) from content type 22 to content type 2. Such a capability could be implemented in an originating IPM 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 IPM or IPN 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 1 - Recommended practices for interworking between 1988 and 1984 MTA implementations are covered in annex D of ISO/IEC ISP 10611-1.

IPM UAs which support both content type 22 and 2 may still receive IPMs which have been downgraded to content type 2, and may receive IPMs containing OR Descriptors and IPM Identifiers copied by 1984 IPM UAs from IPMs whose content has been downgraded. This requires that IPM UAs should treat the downgraded encoding (e.g. of common name) as entirely equivalent to the original encoding.

NOTE 2 - It is not feasible to attempt to reverse the downgrading elsewhere in the MTS, as this would require every message (of content type 2) to be opened and analysed to discover those few which actually contain downgraded encoding to be reversed.

C.2 Downgrading an Interpersonal Message (IPM)

Downgrading of an IPM of content type 22 is as follows.

These rules are also applied recursively to an IPM in a Message body part if the delivered content type of that IPM is known to be 2.

Downgrading of an IPM containing both 1984 and 1988 recipients should only be performed for 1984 recipients (i.e. such an IPM will need to be split).

Any prohibition on implicit conversion or conversion with loss is only concerned with encoded information types and therefore has no impact on any transformation of heading elements.

IECNORM.COM : Click to view the full PDF of ISO/IEC ISP 12062-1:2003

© ISO 2003 — All rights reserved

NOTE – If IPM content type downgrading is provided in the MTS and either Message Origin Authentication Check or Content Integrity Check is present in the envelope, then as a local matter any one of the following options may apply:

a) the presence of these elements may prevent IPM content downgrading being performed;

b) these elements may be verified, IPM content downgrading performed, and these elements re-computed on the downgraded content;

c) these elements may remain unchanged, their presence may be ignored and IPM content downgrading performed;

d) these elements may be deleted from the envelope and IPM content downgrading performed.

C.2.1 Extensions

If the extensions field is present in the heading, or any recipient extensions field is present in a recipient specifier, then each such field is deleted.

C.2.2 OR-Descriptors

If an OR-descriptor contains a formal-name (an OR-name), then the OR-name is downgraded as specified in subclause B.2.7 of ISO/IEC 10021-6.

NOTE - OR-descriptors occur in each of the originator, authorizing-users, primary-recipients, copy-recipients, blind-copy-recipients and reply-recipients heading fields. OR-descriptors also occur in circulation-list-recipients, but C.2.1 deletes this heading extension.

For an originator OR-descriptor, if, after applying these rules, the formal-name has not been downgraded, then downgrading of the content always fails and a non-delivery notification should be returned.

For other OR-descriptors, if, after applying these rules, downgrading has failed, then information from the directory name and/or the original OR-address may be captured in an implementation-defined manner (for example, it may be placed in the free-form-name or in a domain-defined attribute) and the formal-name may then be deleted.

C.2.3 IPM Identifiers

If an IPM identifier contains an OR-name, then the OR-name is downgraded as specified in subclause B.2.7 of ISO/IEC 10021-6.

NOTE - IPM identifiers occur in each of the this-IPM, replied-to-IPM, obsoleted-IPMs and related-IPMs heading fields.

If the OR-name cannot be downgraded, then it is deleted. In such a case, if it is not known that the user-relative-identifier is sufficient on its own for reference purposes, then a string value of "..." should be appended to the user-relative-identifier to indicate that significant information may have been lost. If the result would cause the upper bound to be exceeded, then the “...” string will have to overwrite one or more trailing characters of the original string.

C.2.4 Delivery Envelope

The delivery-envelope, if present in the parameters element of a Message body part, is downgraded according to the following rules. If the delivery-envelope cannot be downgraded, then it is deleted.

If the content-identifier is present, then it is deleted.

If the extensions element is present, then it is deleted.

NOTE 1 - Criticality indicators do not apply.

NOTE 2 - The redirection-history extension should not be transformed into the equivalent format as specified in the suspended 1986 version of MOTIS, since the latter's use of tag [9] conflicts with the use of this tag value for the extensions element in OtherMessageDeliveryFields in ISO/IEC 10021-4.

IECNORM.COM : Click to view the full PDF of ISO/IEC ISP 12062-1:2003

© ISO 2003 — All rights reserved

If the delivered content type is 22, then it is changed to 2.

All OR-names are downgraded as specified in subclause B.2.7 of ISO/IEC 10021-6.

If the originator-name or this-recipient-name cannot be downgraded, then the delivery-envelope cannot be downgraded.

If the originally-intended-recipient-name cannot be downgraded, then either it is deleted or the delivery-envelope cannot be downgraded.

If an other-recipient-name cannot be downgraded, then either that name is deleted or all the other-recipient-names are deleted.

Encoded information types are downgraded as specified in subclause B.2.9 of ISO/IEC 10021-6.

C.2.5 Body

If the syntax element is present in the parameters element of a Videotex body part, then it is deleted.

If an IA5 Text body part or a Message body part is represented as an Extended body part, then it is transformed into the corresponding basic body part type. If an Extended body part is of an body part type other than IA5 Text or Message, and that body part type has a basic body part type defined, then the Extended body part may be transformed into the corresponding basic body part type. Subclause 7.4 of ISO/IEC 10021-7 identifies the equivalences between basic body part types and extended body part types. That list is supplemented by the equivalence for the ODA body part type, as follows:

- ODA extended body part type - defined in annex E of ISO/IEC 8613-1.

- ODA basic body part type - defined in annex B of ISO/IEC ISP 10610-1. Encoded information type bit 0 is set. Bit 10 may additionally be set by bilateral agreement, but may otherwise cause interoperability problems.

These transformations are not considered to be conversion, since they do not affect the semantics of the encoded information types in the message envelope, and hence are not controlled by any prohibition on implicit conversion or conversion with loss.

Any other extended body part types may either be transformed into basic body parts by bilateral agreement, or else downgrading fails. These transformations are considered to be conversion and hence are controlled by any prohibition on implicit conversion or conversion with loss.

NOTE - As such transformation is outside the scope of the conversion rules in the MHS base standards, an implementation may use its own conversion rules. For example, it may encapsulate the complete body part, or alternatively may encapsulate just the data element of the body part. Which body part type is used is a local matter. In the most extreme case, the body part may be replaced with an IA5 Text body part containing an indication of the presence of the original body part, although the objective should be to capture the body part in an encoding compatible with the 1984 standards without loss of information if possible. It should, however, be noted that any associated encoded information types in the message envelope will be mapped to ‘undefined’ according to the rules in annex B of ISO/IEC 10021-6.

C.3 Downgrading an Interpersonal Notification (IPN)

Downgrading of an IPN of content type 22 is as follows.

If the IPN is an Other Notification (ON), then if it contains an advice-notification this may be transformed into an IPM, otherwise downgrading fails.

C.3.1 Extensions

If any of the notification-extensions, rn-extensions or nrn-extensions fields is present, then it is deleted.

IECNORM.COM : Click to view the full PDF of ISO/IEC ISP 12062-1:2003

© ISO 2003 — All rights reserved