INTERNATIONAL STANDARD

ISO/IEC 10021-1

Second edition
2003-11-15

Information technology — Message Handling Systems (MHS)

Part 1: System and service overview

Technologies de l'information — Systèmes de messagerie (MHS)

Partie 1: Présentation générale du système et des services

Reference number
ISO/IEC 10021-1:2003(E)

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

Published in Switzerland

Contents

Page

1 Scope 1

2 Normative references 1

3 Terms and definitions 3
3.1 Open Systems Interconnection 3
3.2 Directory Systems 4

4 Abbreviations 4

5 Conventions 5

6 Purpose 5

7 Functional Model of MHS 5
7.1 Description of the MHS Model 5
7.2 Structure of Messages 6
7.3 Application of the MHS model 7
7.3.1 Physical Mapping 7
7.3.2 Organizational Mapping 8
7.3.3 Administration Management Domain 8
7.3.4 Private Management Domain 8
7.4 The Message Store 9
7.4.1 Physical Configurations 12
7.4.2 Organizational Configurations 12

8 The Message Transfer Service 12
8.1 Submission and Delivery 12
8.2 Transfer 12
8.3 Notifications 12
8.4 User Agent 13
8.5 Message Store 13
8.6 Access Unit 13
8.7 Use of the MTS in the Provision of Various Services 13

9 The IPM Service 13
9.1 IPM Service Functional Model 13
9.2 Structure of IP-messages 13
9.3 IP-notifications 14

10 Intercommunication with Physical Delivery Services 15
10.1 Introduction 15
10.2 Organizational Configurations 16

11 Specialized Access 16
11.1 Introduction 16
11.2 Telex Access 17
11.2.1 Registered Access to the IPM Service 17
11.2.2 Non-registered (Public) Access to the IPM Service 17
11.3 Facsimile Access 17
11.3.1 Non-registered (Public) Access from the IPM Service 17

12 Naming and Addressing 17
12.1 Introduction 17
12.2 Directory Names 17
12.3 OR-Names 18
12.4 OR-Addresses 18

13 MHS Use of Directory 18
13.1 Introduction 18
13.2 Functional Model 19
13.3 Physical Configurations 19

14 Distribution Lists in MHS 20
14.1 Introduction 20
14.2 Properties of a DL 20
14.3 Submission 21
14.4 DL Use of a Directory 21
14.5 DL Expansion 21
14.6 Nesting 21
14.7 Recursion Control 21
14.8 Delivery 21
14.9 Routing Loop Control 21
14.10 Notifications 22
14.11 DL Handling Policy 22

15 Security Capabilities of MHS 22
15.1 Introduction 22
15.2 MHS Security Threats 22
15.2.1 Access Threats 22
15.2.2 Inter-Message Threats 22
15.2.3 Intra-Message Threats 23
15.2.4 Data Store Threats 23
15.3 Security Model 23
15.3.1 Secure Access Management and Administration 23
15.3.2 Secure Messaging 23
15.4 MHS Security Capabilities 24
15.5 Security Management 25
15.6 MHS Security Dependencies 26
15.7 IPM Security 26

16 Conversion in MHS 27

17 *Clause 17 of the corresponding ITU-T Recommendation is not part of this International Standard* 28

18 Elements of Service – Purpose 28

19 Elements of service – Classification 31
19.1 Purpose of Classification 31
19.2 Basic Message Transfer Service 32
19.3 MT Service Optional User Facilities 32
19.4 Base MH/PD Service Intercommunication 34
19.5 Optional User Facilities for MH/PD Service Intercommunication 34
19.6 Base Message Store 34
19.7 MS Optional User Facilities 35
19.8 Basic Interpersonal Messaging Service 35
19.9 IPM Service Optional User Facilities 36

Annex A (informative) Glossary of Terms 40

Annex B (informative) Definitions Of Elements Of Service 55

Annex C (informative) Elements of service changes from 1992 80

Annex D (informative) Differences between ISO/IEC 10021-1 and ITU-T Recommendation X.400 82

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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

ISO/IEC 10021-1 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 6, *Telecommunications and information exchange between systems*.

This part of ISO/IEC 10021 is technically aligned with ITU-T Recommendation F.400/X.400 (1999) but is not published as identical text.

This second edition cancels and replaces the first edition (ISO/IEC 10021-1:1990), which has been technically revised. It also incorporates Technical Corrigenda 1 to 7 and consolidates Amendment 1:1994.

ISO/IEC 10021 consists of the following parts, under the general title *Information technology — Message Handling Systems (MHS)*:

— *Part 1: System and service overview*

— *Part 2: Overall architecture*

— *Part 4: Message transfer system — Abstract service definition and procedures*

— *Part 5: Message store: Abstract service definition*

— *Part 6: Protocol specifications*

— *Part 7: Interpersonal messaging system*

— *Part 8: Electronic Data Interchange Messaging Service*

— *Part 9: Electronic Data Interchange Messaging System*

— *Part 10: MHS routing*

— *Part 11: MHS Routing — Guide for messaging systems managers* [Technical Report]

Introduction

This document is one of a set of Recommendations | International Standards for Message Handling. The entire set provides a comprehensive specification for a Message Handling System (MHS) comprising any number of co-operating open systems.

Message Handling Systems and Services enable users to exchange messages on a store-and-forward basis. A message submitted by one user, the originator, is conveyed by the Message Transfer System (MTS), the principal component of a larger Message Handling System (MHS), and is subsequently delivered to one or more additional users, the message's recipients.

An MHS comprises a variety of interconnected functional entities. Message Transfer Agents (MTAs) co-operate to perform the store-and-forward message transfer function. Message Stores (MSs) provide storage for messages and enable their submission, retrieval and management. User Agents (UAs) help users access MHS. Access Units (AUs) provide links to other communication systems and Services of various kinds (e.g., Telematic Services, Postal Services).

This part of ISO/IEC 10021 specifies the overall system and service description of Message Handling capabilities.

Information technology — Message Handling Systems (MHS) —

Part 1:
System and service overview

1 Scope

This part of ISO/IEC 10021 defines the overall system and service of an MHS and serves as a general overview of MHS.

Other aspects of Message Handling Systems and Services are defined in other parts of ISO/IEC 10021. The structure of ISO/IEC 10021 (all parts) defining the Message Handling System and Services is shown in Table 1.

The technical aspects of MHS are defined in other parts of ISO/IEC 10021. The overall system architecture of MHS is defined in ISO/IEC 10021-2:2003.

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.

ISO/IEC 7498-1:1994, *Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model*

ISO/IEC 8649:1996, *Information technology – Open Systems Interconnection – Service definition for the Association Control Service Element*

ISO/IEC 8824-1:1998, *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation*

ISO/IEC 8825-1:1998, *Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*

ISO/IEC 9066-1:1989, *Information processing systems – Text communication – Reliable Transfer – Part 1: Model and service definition*

ISO/IEC 13712-1:1995, *Information technology – Remote Operations: Concepts, model and notation*

ISO/IEC 9594 (all parts), *Information technology – Open Systems Interconnection – The Directory*

ISO/IEC 10021-2:2003, *Information technology – Message Handling Systems (MHS) – Part 2: Overall architecture*

ISO/IEC 10021-4:2003, *Information technology – Message Handling Systems (MHS) – Part 4: Message transfer system: Abstract service definition and procedures*

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

ISO/IEC 10021-6:2003, *Information technology – Message Handling Systems (MHS) – Part 6: Protocol specifications*

ISO/IEC 10021-7:2003, *Information technology – Message Handling Systems (MHS) – Part 7: Interpersonal messaging system*

ISO/IEC 10021-8:1999, *Information technology – Message Handling Systems (MHS) – Part 8: Electronic Data Interchange Messaging Service*

ISO/IEC 10021-9:1999, *Information technology – Message Handling Systems (MHS) – Part 9: Electronic Data Interchange Messaging System*

ISO/IEC 10021-10:1999, *Information technology – Message Handling Systems (MHS) – Part 10: MHS routing*

ISO/IEC 10021-11:1999, *Information technology – Message Handling Systems (MHS) – Part 11: MHS Routing – Guide for messaging systems managers*

ISO/IEC 11588-1:1996, *Information technology – Message Handling Systems (MHS) management – Part 1: Model and architecture*

ISO/IEC 11588-3:1997, *Information technology – Message Handling Systems (MHS) management – Part 3: Logging information.*

ISO/IEC 11588-8:1997, *Information technology – Message Handling Systems (MHS) management – Part 8: Message Transfer Agent management.*

CCITT Recommendation F.423:1992, *Message handling services: Intercommunication between the interpersonal messaging service and the telefax service*

CCITT Recommendation F.440:1992, *Message handling services: The voice messaging service*

CCITT Recommendation T.330:1988, *Telematic access to interpersonal messaging system*

CCITT Recommendation X.408 (1988), *Message handling systems: Encoded information type conversion rules*

CCITT Recommendation X.440 (1992), *Message handling systems: Voice messaging system*

Table 1 – Structure of MHS Standards

Short title	Joint MHS		Joint support		ITU-T only	
	ISO/IEC	ITU-T	ISO/IEC	ITU-T	System	Service
MHS: System and service overview	10021-1	X.400				F.400
MHS: Overall architecture	10021-2	X.402				
MHS: Encoded information type conversion rules					X.408	
MHS: MTS: Abstract service definition and procedures	10021-4	X.411				
MHS: MS: Abstract -service definition	10021-5	X.413				
MHS: Protocol specifications	10021-6	X.419				
MHS: Interpersonal messaging system	10021-7	X.420				
Telematic Access to IPMS						
MHS: EDI messaging service	10021-8	F.435			T.330	
MHS: EDI messaging system	10021-9	X.435				
MHS: Voice messaging service						
MHS: Voice messaging system					F.440	
MHS: Routing	10021-10	X.412			X.440	
MHS: Routing: Guide for Messaging System Managers	10021-11	X.404				
MHS: Naming and addressing for public MH services						F.401
MHS: The public message transfer service						F.410
MHS: Intercommunication with public physical delivery services						F.415
MHS: The public IPM service						F.420
MHS: Intercommunication between IPM service and Telex						F.421
MHS: Intercommunication between IPM service and Telefax						F.423
OSI: Basic Reference Model			7498-1	X.200		
OSI: Specification of Abstract Syntax Notation One (ASN.1)			8824-1	X.680		
OSI: Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1)			8825-1	X.690		
OSI: Association Control: Service Definition			8649	X.217		
OSI: Association Control: Protocol Specification			8650-1	X.227		
OSI: Reliable Transfer: Model and service definition			9066-1	X.218		
OSI: Reliable Transfer: Protocol Specification			9066-2	X.228		
OSI: Remote Operations: Concepts, Model & Notation			13712-1	X.880		
OSI: Remote Operations: Service Definition			13712-2	X.881		
OSI: Remote Operations: Protocol Specification			13712-3	X.882		

3 Terms and definitions

For the purposes of this document, the terms and definitions given in Annex A and the following apply.

3.1 Open Systems Interconnection

This part of ISO/IEC 10021 makes use of the following terms defined in ISO/IEC 7498-1:

a) Application Layer;

b) application-process;

c) Open Systems Interconnection;

d) OSI Reference Model.

3.2 Directory Systems

This part of ISO/IEC 10021 makes use of the following terms defined in ISO/IEC 9594-1:

a) directory entry;
b) directory system agent;
c) Directory System;
d) directory user agent.

This part of ISO/IEC 10021 makes use of the following terms defined in ISO/IEC 9594-2:

e) attribute;
f) group;
g) name.

4 Abbreviations

A	Additional
ADMD	Administration Management Domain
AU	Access Unit
CA	Contractual Agreement
DL	Distribution List
DSA	Directory System Agent
DUA	Directory User Agent
E	Essential
EDI	Electronic Data Interchange
EIT	Encoded Information Type
I/O	Input/Output
IP	Interpersonal
IPM	Interpersonal Messaging
IPMS	Interpersonal Messaging System
MD	Management Domain
MH	Message Handling
MHS	Message Handling System
MS	Message Store
MT	Message Transfer
MTA	Message Transfer Agent
MTS	Message Transfer System
N/A	Not applicable
OR	Originator/Recipient
OSI	Open Systems Interconnection
PD	Physical Delivery
PDAU	Physical Delivery Access Unit
PDS	Physical Delivery System
PM	Per-message
PR	Per-recipient
PRMD	Private Management Domain

PTLXAU	Public Telex Access Unit
RPOA	Recognized Private Operating Agency
TLMA	Telematic Agent
TLXAU	Telex Access Unit
UA	User Agent

5 Conventions

In this Standard, the expression "Administration" is used to indicate a telecommunication Administration, a recognized private operating agency, and, in the case of intercommunication with Public Delivery Service, a Postal Administration.

6 Purpose

This part of ISO/IEC 10021 is one of a set of Recommendations which describes the system model and elements of service of the Message Handling System (MHS) and Services. This part of ISO/IEC 10021 overviews the capabilities of an MHS that are used for the provision of MH Services to enable users to exchange messages on a store-and-forward basis.

The message handling system is designed in accordance with the principles of the Reference Model of Open Systems Interconnection (OSI Reference Model) (ISO/IEC 7498-1) and uses the Presentation Layer Services and Services offered by other, more general, Application Service Elements. An MHS can be constructed using any network fitting in the scope of OSI. The Message Transfer Service provided by the MTS is application independent. An example of a standardized application is the IPM service. End systems can use the MT Service for specific applications that are defined bilaterally.

Elements of Service are the service features provided through the Application Processes. The Elements of Service are considered to be components of the services provided to users and are either elements of a basic service or they are *optional user facilities*, classified either as *essential optional user facilities*, or as *additional optional user facilities*.

7 Functional Model of MHS

The MHS functional model serves as a tool to aid in the development of International Standards for MHS, and aids in describing the basic concepts that can be depicted graphically. It comprises several different functional components that work together to provide MH services. The model can be applied to a number of different physical and organizational configurations.

7.1 Description of the MHS Model

A functional view of the MHS model is shown in Figure 1. In this model, a user is either a person or a computer process. Users are either direct users (i.e. engage in message handling by direct use of MHS), or are indirect users [i.e. engage in message handling through another communication system (e.g. a physical delivery system) that is linked to MHS]. A user is referred to as either an originator (when sending a message) or a recipient (when receiving a message). Message Handling Elements of Service define the set of message types and the capabilities that enable an originator to transfer messages of those types to one or more recipients.

An originator prepares messages with the assistance of his User Agent. A User Agent (UA) is an application process that interacts with the Message Transfer System (MTS) or a Message Store (MS), to submit messages on behalf of a single user. The MTS delivers the messages submitted to it, to one or more recipient UAs, Access Units (AUs), or MSs, and can return notifications to the originator. Functions performed solely by the UA and not standardized as part of the message handling Elements of Service are called local functions. A UA can accept delivery of messages directly from the MTS, or it can use the capabilities of an MS to receive delivered messages for subsequent retrieval by the UA.

The MTS comprises a number of Message Transfer Agents (MTAs). Operating together, in a store-and-forward manner, the MTAs transfer messages and deliver them to the intended recipients.

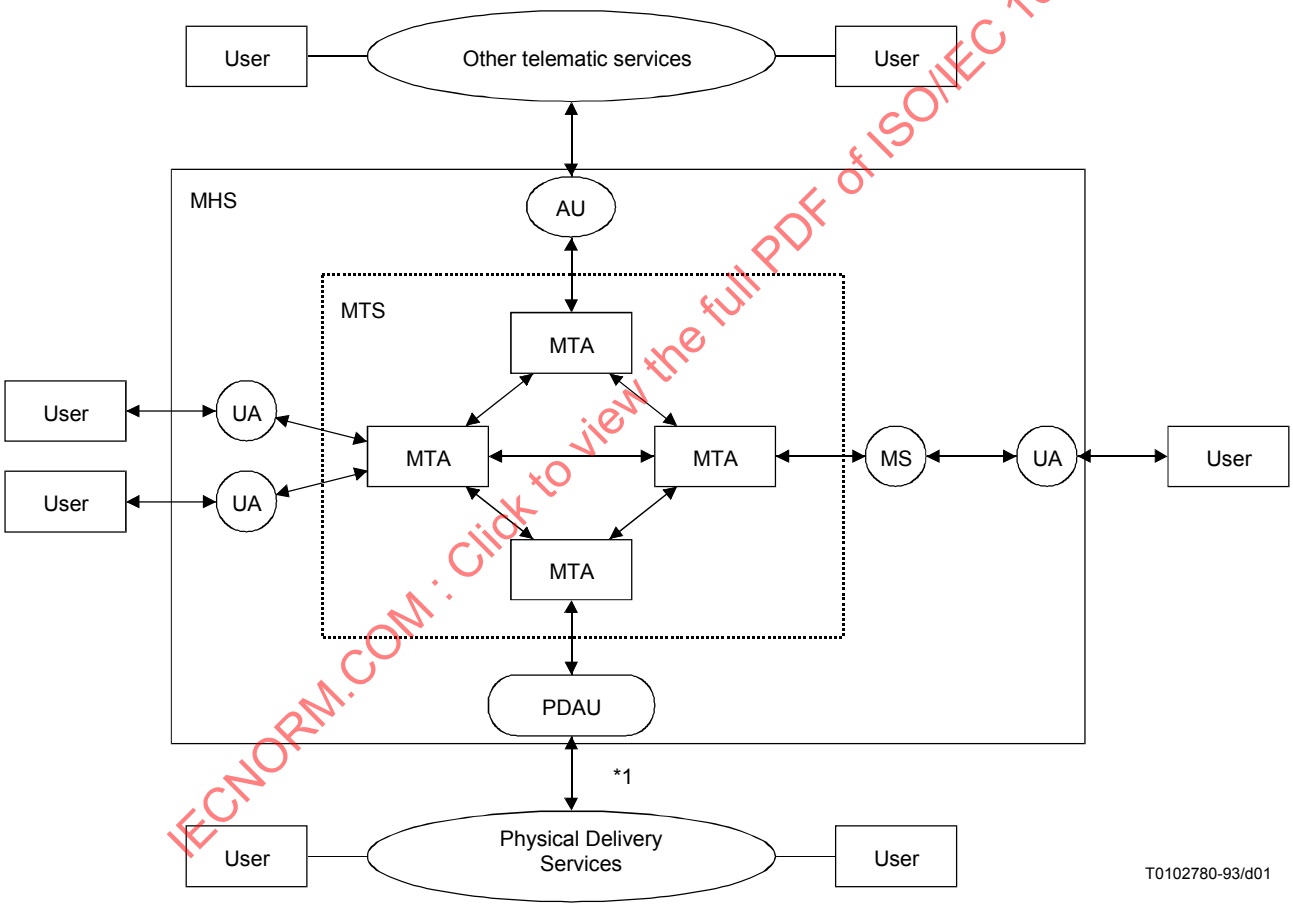
Access by indirect users of MHS is accomplished by AUs. Delivery to indirect users of MHS is accomplished by AUs, such as in the case of physical delivery, by the Physical Delivery Access Unit (PDAU).

The Message Store (MS) is an optional general purpose capability of MHS that acts as an intermediary between the UA and the MTA. The MS is depicted in the MHS Functional Model as shown in Figure 1. The MS is a functional entity whose primary purpose is to store delivered, and, optionally, submitted messages and permit their retrieval by the MS-user (UA). The MS also allows for submission from, and alerting to the MS-user.

The collection of UAs, MSs, AUs and MTAs is called the Message Handling System (MHS).

7.2 Structure of Messages

The basic structure of messages conveyed by the MTS is shown in Figure 2. A message is made up of an envelope and a content. The envelope carries information that is used by the MTS when transferring the message within the MTS. The content is the piece of information that the originating UA wishes to be delivered to one or more recipient UAs. The MTS neither modifies nor examines the content, except for conversion (see clause 16).



* 1) Message input from PDS to MHS is not currently possible. Flow from PD services to the PDAU shown is for the purpose of notifications.

Figure 1 – MHS Functional Model

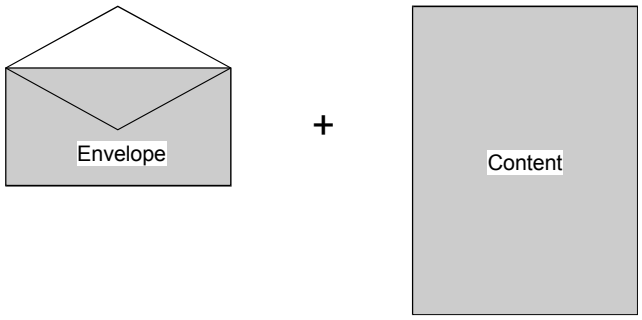


Figure 2 – Basic Message Structure

7.3 Application of the MHS model

7.3.1 Physical Mapping

Users access UAs for message processing purposes, for example, to create, present, or file messages. A user can interact with a UA via an input/output (I/O) device or process (e.g. keyboard, display, printer etc.). A UA can be implemented as a (set of) computer process(es) in an intelligent terminal.

A UA and MTA can be co-located in the same system, or a UA/MS can be implemented in physically separate systems. In the first case the UA accesses the MT Elements of Service by interacting directly with the MTA in the same system. In the second case, the UA/MS will communicate with the MTA via standardized protocols specified for MHS. It is also possible for an MTA to be implemented in a system without UAs or MSs.

Some possible physical configurations are shown in Figures 3 and 4. The different physical systems can be connected by means of dedicated lines or switched network connections.

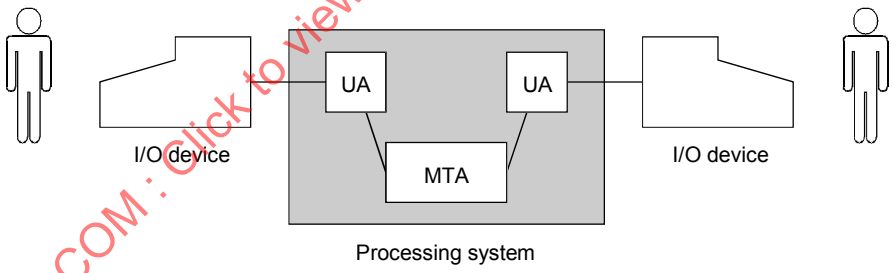


Figure 3 – Co-resident UA and MTA

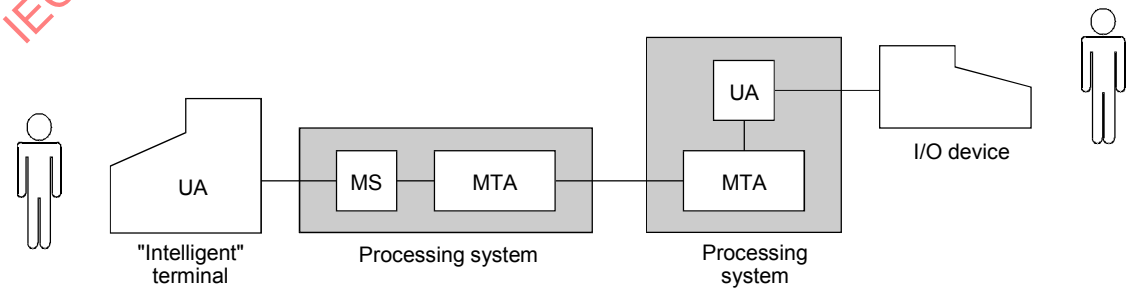


Figure 4 – Stand-alone UA and Co-resident MS/MTA and UA/MTA

7.3.2 Organizational Mapping

An Administration or organization can play various roles in providing Message Handling Services. An organization in this context can be a company or a non-commercial enterprise.

The collection of at least one MTA, zero or more UAs, zero or more MSs, and zero or more AUs constitutes a Management Domain (MD). An MD provides Message Handling Services in accordance with the classification of Elements of Service as described in clause 19. A Management Domain may be classified as either an Administration Management Domain (ADMD) or a Private Management Domain (PRMD) with the definitions given in Annex A. The relationship between Management Domains is shown in Figure 5.

7.3.3 Administration Management Domain

In one country, one or more ADMDs can exist. An ADMD is characterized by its provision of relaying functions between other Management Domains and the provision of the Message Transfer Service for the applications provided within the ADMD.

An Administration can provide access for its users to the ADMD in one or more of the following ways:

– user to Administration provided UA;
– private UA to Administration MTA;
– private UA to Administration MS;
– private MTA to Administration MTA;
– user to Administration provided AU.

See also the examples of configurations shown in Figures 3 and 4.

Administration provided UAs can exist as part of an intelligent terminal that the user can use to access MHS. They can also exist as part of Administration resident equipment being part of MHS, in which case the user obtains access to the UA via an I/O device.

In the case of a private UA, the user has a private stand-alone UA which interacts with the Administration provided MTA or MS, using submission, delivery and retrieval functions. A private, stand-alone UA can be associated with one or more MDs, provided that the required naming conventions are preserved.

A private MTA as part of a PRMD can access one or more ADMDs in a country, following national regulations.

Access can also be provided by Administration provided AUs described in clauses 10 and 11.

7.3.4 Private Management Domain

An organization other than an Administration can have one or more MTA(s), and zero or more UAs, AUs and MSs forming a PRMD which can interact with an ADMD or other PRMD on an MD-to-MD (MTA-to-MTA) basis. A PRMD is characterized by the provision of messaging functions within that Management Domain.

A PRMD can have access to one or more ADMDs as shown in Figure 5. However, in the case of a specific interaction between a PRMD and an ADMD (such as when a message is transferred between MDs), the PRMD is considered to be associated only with that ADMD. A PRMD may act as a relay to other MDs if national regulations and bilateral agreements permit.

As a national matter, the name of a PRMD can be either nationally unique or relative to the associated ADMD. If a PRMD is associated with more than one ADMD, the PRMD can have more than one name.

See Annex G of ISO/IEC 10021-2 for guidance in the case of multinational PRMDs.

7.4 The Message Store

Remote UAs can be implemented on a wide variety of equipment, including personal computers of varying capabilities. The MS service can complement a remote UA by providing continuously available storage and delivery services on behalf of a user, for example.

One MS acts on behalf of only one user, i.e. it does not provide a common or shared MS capability to several users. See also PRMD 3 of Figure 5.

The MS will store delivered messages and reports. As an option it may also store submitted messages, submitted probes, and draft messages. The MS may also keep a history of messages by storing extracts of previously and currently stored messages in logs. Messages may be grouped in a user-defined and potentially hierarchical structure.

The MS retrieval capability provides users who subscribe to an MS with basic message retrieval capabilities potentially applicable to all information held by the MS. Figure 6 shows the delivery, and subsequent retrieval of messages that are delivered to an MS, and the submission of messages via the MS.

When a user subscribes to an MS, all messages destined for the user are delivered to the MS only. The MS-user, if on line, may receive Alerts that announce the delivery of certain messages to the MS. Messages delivered to an MS are considered delivered from the MTS perspective.

The basic MS is independent of application specific services (see 8.7) and may store messages with all types of content, the type of content being dependent on the type of service. However, it may provide additional capabilities depending on the type of content.

When an MS-user submits a message, the MS conveys the submission request to the MTS and reports the outcome returned by the MTS to the MS-user. If requested by the MS-user, the MS may expand the message by forwarding parts of delivered or submitted messages that are currently stored in the MS before conveying the submission to the MTS. The MS may also store a copy of the message submitted to the MTS if the submission is successful. The MS service allows the user to transfer a message to the MS for storage as a draft message. The draft message may subsequently be retrieved, or the MS may include its body-parts in a message submitted to the MTS when requested in a message submitted by the MS-user.

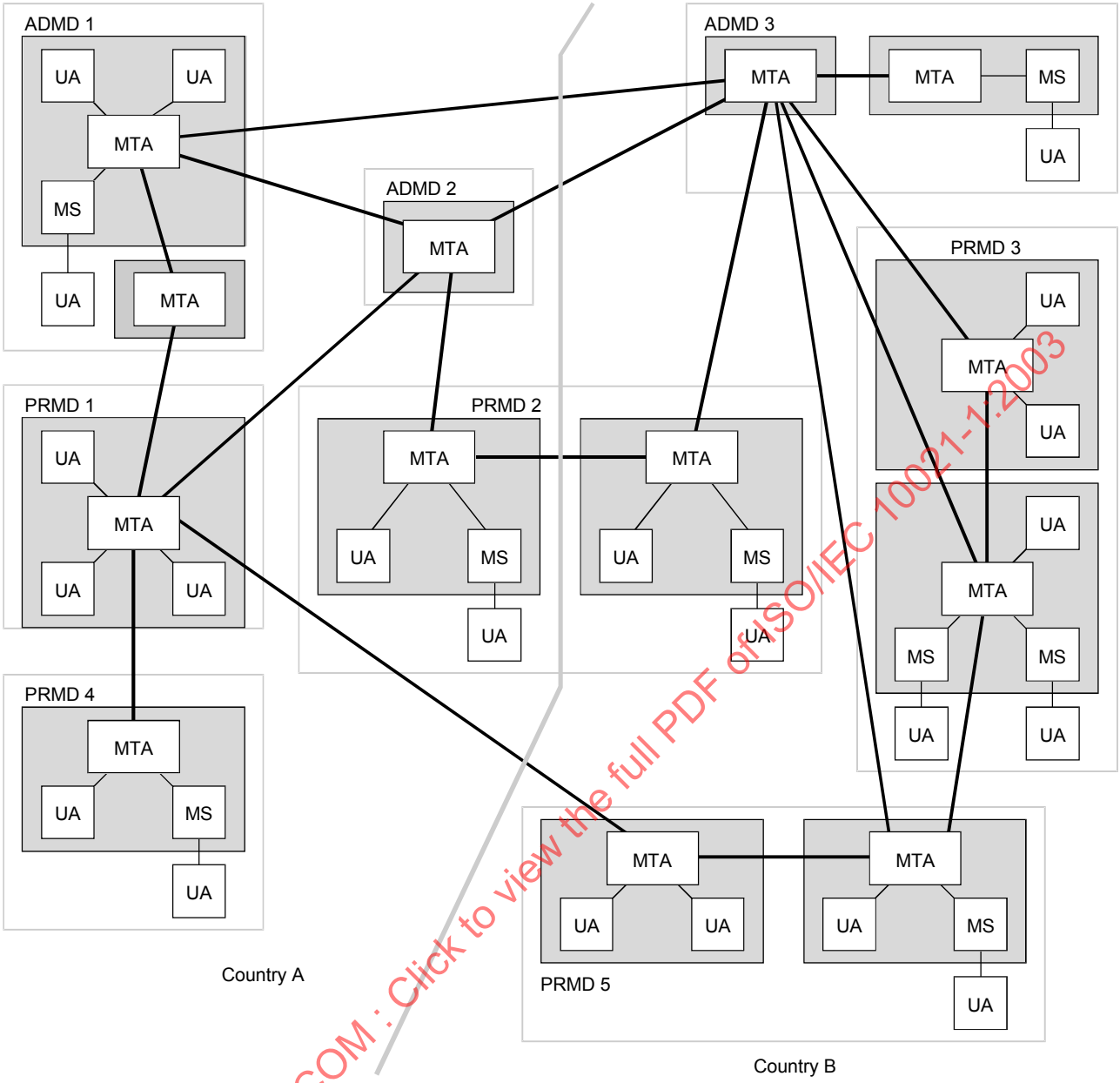
The MS-user may be provided with the capability to request the MS service to forward selected messages automatically upon delivery. The MS may also provide automatic deletion of messages after a user specified period of time, or when the message expires, or when the message is rendered obsolete by another message.

The MS may automatically attach information to a previously submitted message concerning its delivery or non-delivery. The MS may also generate content-specific notifications, acknowledging receipt or acceptance when requested by the user or when the user has retrieved the message.

The elements of service describing the features of the MS are defined in Annex B and classified in clause 19. Users are provided with the capability based on various criteria, to get counts and lists of messages, to fetch messages, and to delete messages, currently held in the MS.

Figure 7 depicts a simplified model of the information types stored in the MS, and the functions the MS fulfils.

The scope of the MS services defined in CCITT Recommendation F.400 (1988) and (1992) | ISO/IEC 10021-1:1990 was mainly limited to the storage of delivered messages and reports and their subsequent retrieval by the MS-user. The 1994 version of this part of ISO/IEC 10021 defines new extensions to provide a broader range of service facilities. These enhanced facilities particularly apply in those environments where the MS is used as a personal data base to store, retrieve, modify, and classify a user's messages, often with frequent and long-lasting interaction between the MS-user and MS. Examples of such environments might be found in local area networks, or in environments where the user employs different User Agent implementations at different locations to access one MS. In other environments where the MS is used mainly as a temporary storage system, to take delivery of messages and reports and provide for their retrieval by infrequent and short-lasting interactions, these enhanced facilities may not be required. In this latter case, some enhanced facilities may be provided locally by the MS-user itself.



NOTE 1 – This diagram gives examples of possible interconnections. It does not attempt to identify all possible configurations. This International Standard places no restrictions on interconnections between MDs, although these may be the subject of regulatory agreements within and between countries.

NOTE 2 – PRMD 1 has connections to two ADMDs within country A;
– PRMD 2 spans a country border, and has connections to an ADMD in each country;
– PRMD 3 has multiple connections to ADMD 3;
– PRMD 4 is only connected to other MDs by relaying through PRMD 1;
– PRMD 5 has connections to other PRMDs, both within the same country (to PRMD 3) and internationally (to PRMD 1).

NOTE 3 – The lines between MTAs represent logical connections, which implies that the MTAs have the ability to establish associations between themselves when required, using supporting OSI layers over any physical medium.

NOTE 4 – The shaded boxes surrounding logical components (e.g. UAs, MTAs) represent examples of physically colocated systems.

Figure 5 – Relationships between Management Domains

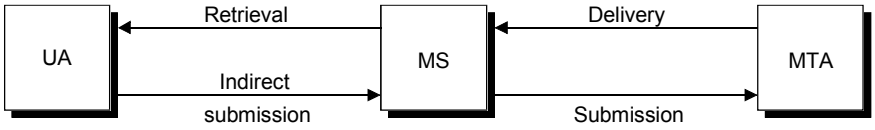
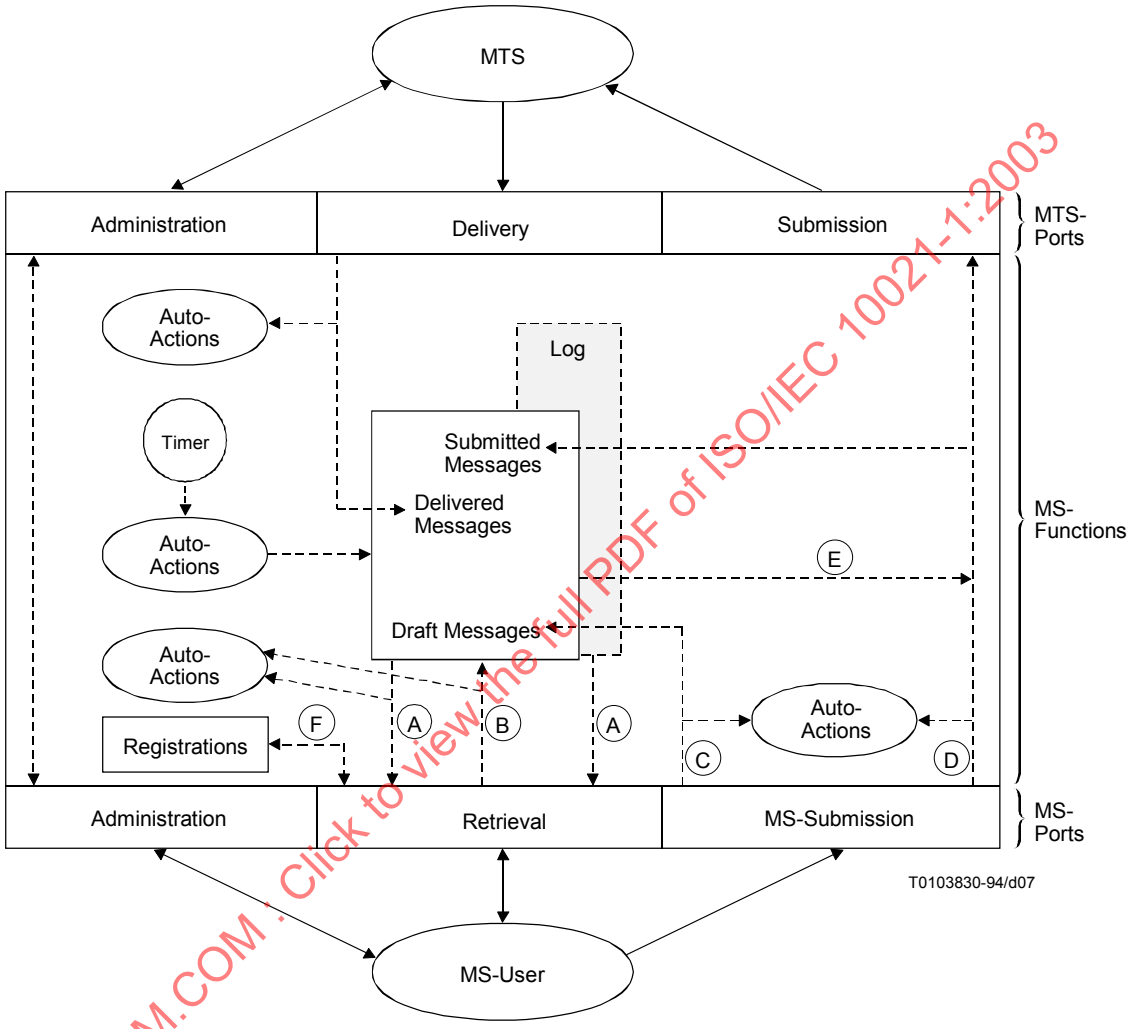


Figure 6 – Submission & Delivery with an MS



(A) Fetch, list and summarize
(B) Modify message attributes and
(C) Draft storage
(D) Submission to the MTS
(E) Submission to the MTS with incorporation of parts of stored
(F) Register-MS

Figure 7 – Message Store Functional Model

Consequently, the basic and essential optional requirements defined for the MS in this part of ISO/IEC 10021 are the same as those defined in versions published prior to 1994.

7.4.1 Physical Configurations

The MS can be physically located with respect to the MTA in a number of ways. The MS can be co-located with the UA, co-located with the MTA, or stand-alone. From an external point of view, a co-located UA and MS are indistinguishable from a stand-alone UA. Co-locating the MS with the MTA offers significant advantages which will probably make it the predominant configuration.

7.4.2 Organizational Configurations

Either ADMDs or PRMDs can operate MSs. All the subscriber's messages are delivered to the MS for subsequent retrieval.

The physical and organizational configurations described above are examples only and other equally valid cases can exist.

8 The Message Transfer Service

The MTS provides the general, application independent, store and forward Message Transfer service. The Elements of Service describing the features of the MT service are defined in Annex B, and classified in clause 19.

8.1 Submission and Delivery

The MTS provides the means by which UAs exchange messages. There are two basic interactions between MTAs and UAs, or AUs, or MSs:

1) The submission interaction is the means by which an originating UA or MS transfers to an MTA the content of a message and the submission envelope. The submission envelope contains the information that the MTS requires to provide the requested Elements of Service.

2) The delivery interaction is the means by which the MTA transfers to a recipient UA or MS the content of a message plus the delivery envelope. The delivery envelope contains information related to delivery of the message.

In the submission and delivery interactions, responsibility for the message is passed between the MTA and the UA or MS.

8.2 Transfer

Starting at the originator's MTA, each MTA transfers the message to another MTA until the message reaches the recipients' MTA, which then delivers it to the recipient UA or MS using the delivery interaction.

The transfer interaction is the means by which one MTA transfers to another MTA the content of a message plus the transfer envelope. The transfer envelope contains information related to the operation of the MTS plus information that the MTS requires to provide Elements of Service requested by the originating UA.

MTAs transfer messages containing any type of binary coded information. MTAs neither interpret nor alter the content of messages except when performing a conversion.

8.3 Notifications

Notifications in the MT Service comprise the Delivery and Non-delivery Notifications. When a message, or Probe, cannot be delivered by the MTS, a Non-delivery Notification is generated and returned to the originator in a Report signifying this. In addition, an originator can specifically ask for acknowledgment of successful delivery through use of the Delivery Notification Element of Service on submission.

8.4 User Agent

The UA uses the MT service provided by the MTS. A UA is a functional entity by means of which a single direct user engages in message handling.

UAs are grouped into classes based on the type of content of messages they can handle. The MTS provides a UA with the ability to identify its class when sending messages to other UAs. UAs within a given class are referred to as cooperating UAs since they cooperate with each other to enhance the communication amongst their respective users.

NOTE – A UA can support more than one type of message content, and hence belong to several UA classes.

8.5 Message Store

The Message Store (MS) uses the MT Service provided by the MTS. An MS is a functional entity associated with a user's UA. The user may submit messages through the MS and retrieve messages that have been either delivered to the MS, or submitted by the user.

8.6 Access Unit

An Access Unit (AU) uses the MT service provided by the MTS. An AU is a functional entity associated with an MTA to provide for intercommunication between the MHS and another system or service.

8.7 Use of the MTS in the Provision of Various Services

The MTS is used by application specific services for the provision of Message Handling Services of various types. The Interpersonal Messaging Service, described in clause 9, is one example of this. Other examples are the Electronic Data Interchange (EDI) messaging service described in CCITT Rec. F.435 | ISO/IEC 10021-8, and the Voice Messaging service described in CCITT Rec. F.440. Other services can be built on the foundation of the MTS, either with corresponding standards or as private applications.

9 The IPM Service

The Interpersonal Messaging Service (IPM Service) provides a user with features to assist in communicating with other IPM Service users. The IPM Service uses the capabilities of the MT Service for sending and receiving interpersonal messages. The Elements of Service describing the features of the IPM Service are defined in Annex B, and classified in clause 19.

9.1 IPM Service Functional Model

Figure 8 shows the functional model of the IPM Service. The UAs used in the IPM Service (IPM-UAs) comprise a specific class of cooperating UAs. The optional Access Units shown (PFAXAU, PTLXAU, TLMA) allow for Telex, and TeleFax users to intercommunicate with the IPM Service. The optional Physical Delivery Access Unit (PDAU) allows IPM users to send messages to users outside the IPM Service who have no access to MHS. The Message Store can optionally be used by IPM users to take delivery of messages on their behalf.

9.2 Structure of IP-messages

The IPM class of UAs create messages containing a content specific to the IPM. The specific content that is sent from one IPM-UA to another is a result of an originator composing and sending a message, called an IP-message. The structure of an IP-message as it relates to the basic message structure of MHS is shown in Figure 9. The IP-message is conveyed with an envelope when being transferred through the MTS.

Figure 10 shows an analogy between a typical office memo, and the corresponding IP-message structure. The IP-message contains information (e.g. To, cc, Subject) provided by the user which is transformed by the IPM-UA into the heading of the IP-message. The main information that the user wishes to communicate (the body of the memo) is contained within the body of the IP-message. In the example shown, the body contains two types of encoded information: text and facsimile, which form what are called, body parts. In general, an IP-message body can consist of a number of body parts, each of which can be of a different encoded information type, such as voice, text, files, facsimile and graphics.

9.3 IP-notifications

In the IPM Service, a user can request a notification of receipt or non-receipt of a message by a recipient. These notifications are requested by an originator and are generated as a result of some recipient action (such as reading/not reading the message). In certain cases, the Non-receipt Notification is generated automatically by the recipient's UA.

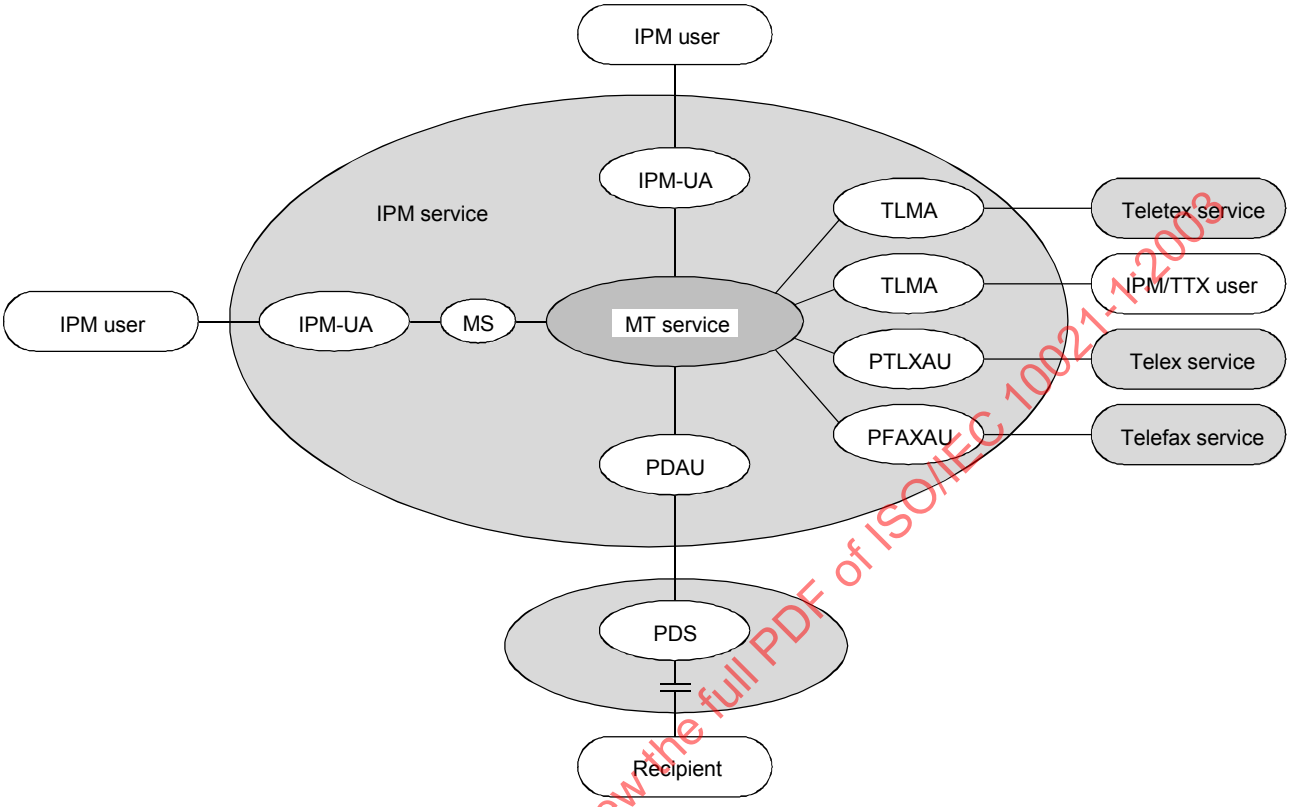


Figure 8 – IPM Service Functional Model

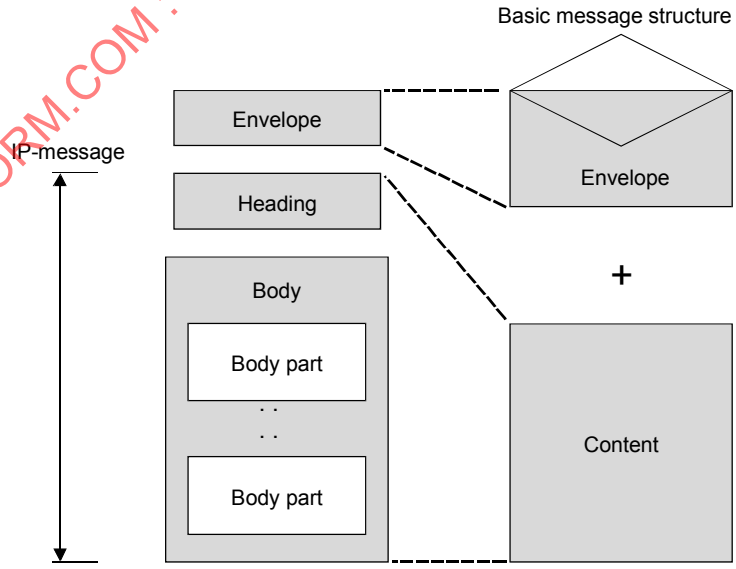


Figure 9 – IP-message Structure

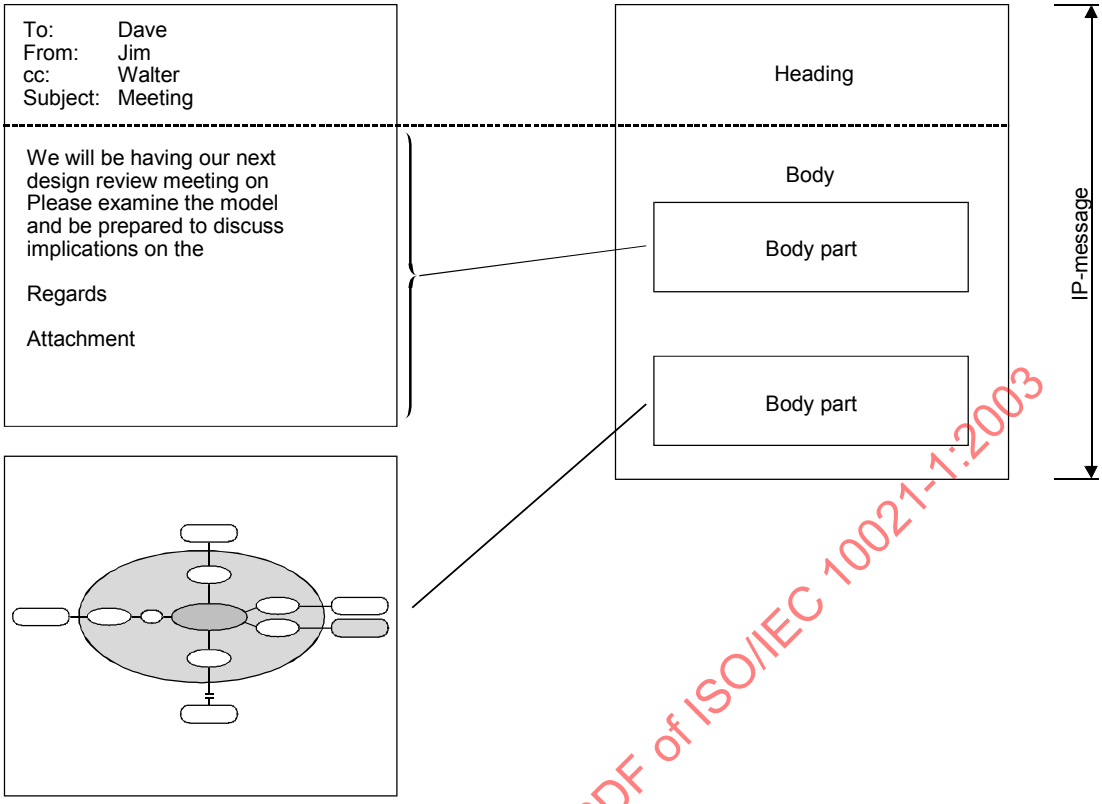


Figure 10 – IP-message Structure For a Typical Memo

10 Intercommunication with Physical Delivery Services

10.1 Introduction

The value of Message Handling Systems can be increased by connecting them to Physical Delivery (PD) Systems such as the traditional Postal Service. This will allow for the physical (e.g. hard copy) delivery of messages originated within MHS to recipients outside of MHS, and in some cases will allow for the return of notifications from the PD service to an MHS originator. The ability for origination of messages in the PD service for submission to MHS through the PDAU is not yet provided. The capability of intercommunication between PD and MH services is an optional capability of MHS, and is applicable to any application such as IPM. All users of MHS will have the ability to generate messages for subsequent physical delivery. Figure 11 shows the functional model of this interworking. The Elements of Service describing the features of this intercommunication are defined in Annex B and classified in clause 19.

A Physical Delivery System is a system, operated by a Management Domain, that transports and delivers physical messages. A physical message is a physical object comprising a relaying envelope and its content. An example of a PDS is the postal service. An example of a physical message is a paper letter and its enclosing paper envelope.

A Physical Delivery Access Unit (PDAU) converts an MH user's message to physical form, a process called physical rendition. An example of this is the printing of a message and its automatic enclosure in a paper envelope. The PDAU passes the physically rendered message to a PDS for further relaying and eventual physical delivery.

A PDAU can be viewed as a set of UAs, each UA being identified by a postal address. To perform its functions, a PDAU must support submission (Notifications) and delivery interactions with the MTS, and also cooperate with other UAs. MH/PD Service intercommunication is thus provided as part of the Message Transfer Service.

To enable MH users to address messages to be delivered physically by a PDS, an appropriate address form appropriate for this exists and is described in clause 12.

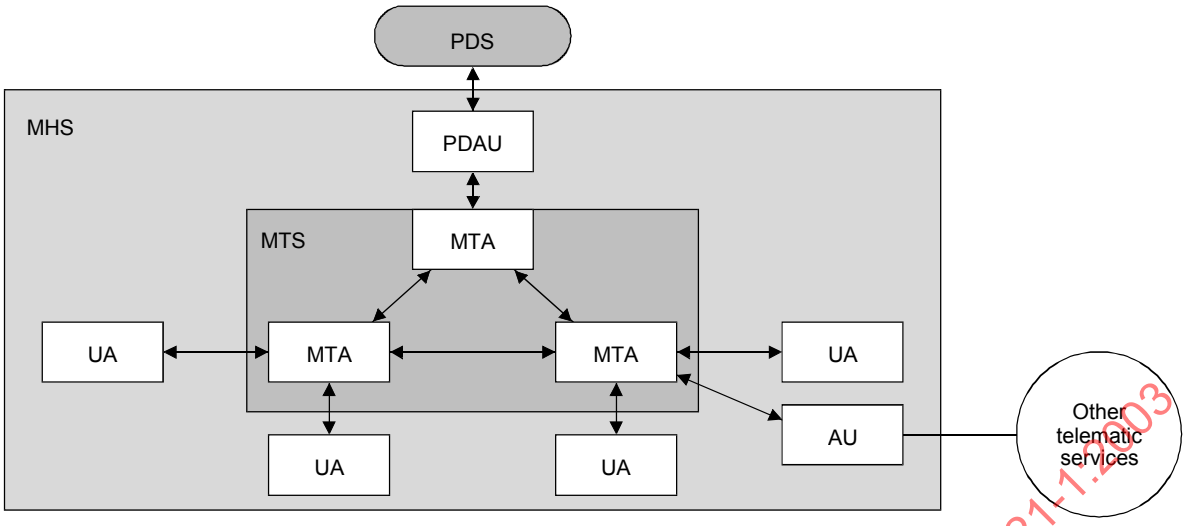


Figure 11 – Functional Model MHS-PDS

10.2 Organizational Configurations

Possible organizational mappings of the functional model described above are shown in Figure 12. In each model (A and B), the term PD domain denotes the domain of responsibility of an organization providing a PD service. In A, the PD domain comprises an MD and a PDS. The boundary between the PD domain and the rest of MHS is a boundary between MDs. In B, the PD domain comprises only the PDS; the PDAU is not part of the PD domain. The boundary between the PD domain and MHS lies at the point where the PDAU passes physical messages to the PDS.

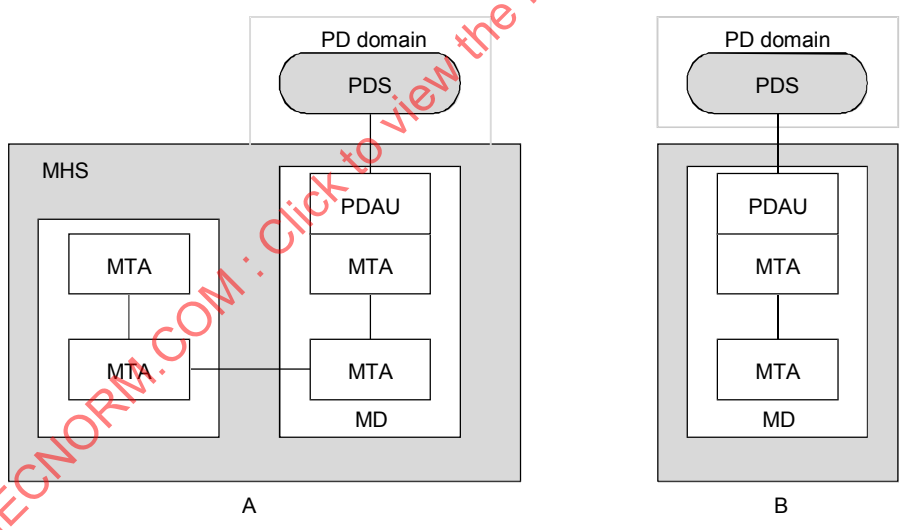


Figure 12 – Configurations for MH/PD Service Intercommunication

11 Specialized Access

11.1 Introduction

The functional model of MHS (see Figure 1) contains Access Units (AUs) to allow access between MHS and other communication systems and services. The model shows a generic Access Unit between MHS and Telematic Services.

Also shown is a Physical Delivery Access unit to allow for physical delivery of MHS messages to recipients without the need for terminal access to MHS. The access to Physical Delivery Services is available to any application carried by the MTS, through a PDAU described in clause 10.

Other forms of access are described below.

NOTE – The use of the word "public" in these descriptions refers only to the concept of unrestricted access by any user without advanced registration, in contrast to registered use. The term is not intended to imply that these access units are only provided as part of a public service; they may equally be provided within a private system.

11.2 Telex Access

11.2.1 Registered Access to the IPM Service

A Telex Access Unit (TLXAU) is defined in the technical Recommendations to allow the intercommunication between IPM users and Telex users. To provide a service with this type of AU is a national matter.

11.2.2 Non-registered (Public) Access to the IPM Service

A specialized Access Unit is defined to allow the intercommunication between IPM users and Telex users. This AU provides for public access to the IPM Service for Telex users who are not registered users of the IPM Service, and is called a Public Telex Access Unit (PTLXAU). This is shown in Figure 8. The Telex users are not subscribers to the IPM Service, but use some of the features of the IPM Service to pass messages to IPM users. IPM users can also send messages to Telex users via this AU.

11.3 Facsimile Access

11.3.1 Non-registered (Public) Access from the IPM Service

A specialized access unit is defined to allow the intercommunication between IPM users and Fascimile users. This AU provides for access from the IPM Service to Fax users who are not registered users of the IPM Service, and is called a Public Fax Access Unit (PFAXAU). This is shown in Figure 8. IPM users can send messages to Fax users via this AU. Operation of the PFAXAU in the direction Fax to IPM is for further study.

12 Naming and Addressing

12.1 Introduction

In an MHS, the principal entity that requires naming is the user (the originator and recipient of messages). In addition, distribution lists (DLs) have names for use in MHS. Users of MHS and DLs are identified by OR-names. OR-names are comprised of directory names and/or OR-addresses, all of which are described in this clause.

12.2 Directory Names

Users of the MH Service, and DLs, can be identified by a name, called a directory name. A directory name must be looked up in a directory to find out the corresponding OR-address. The structure and components of directory names are described in ISO/IEC 9594.

A user can access a directory system directly to find the OR-address of a user, or OR-addresses of the members of a DL (both of which are outside the scope of these Recommendations). As an alternative, a user can use the directory name and have MHS access a directory to resolve the corresponding OR-address or addresses automatically as described in clause 14.

An MH user or DL will not necessarily have a directory name, unless they are registered in a directory. As directories become more prevalent, it is expected that directory names will be the preferred method of identifying MHS users to each other.

12.3 OR-Names

Every MH user or DL will have one or more OR-name(s). An OR-name comprises a directory name, an OR-address, or both.

Either or both components of an OR-name can be used on submission of a message. If only the directory name is present, MHS will access a directory to attempt to determine the OR-address, which it will then use to route and deliver the message. If a directory name is absent, it will use the OR-address as given. When both are given on submission, MHS will use the OR-address, but will carry the directory name and present both to the recipient. If the OR-address is invalid, it will then attempt to use the directory name as above.

12.4 OR-Addresses

An OR-address contains information that enables MHS to uniquely identify a user to deliver a message or return a notification to him. (The prefix "OR" recognizes the fact that the user can be acting as either the originator or recipient of the message or notification in question.)

An OR-address is a collection of information called attributes. ISO/IEC 10021-2 specifies a set of standard attributes from which OR-addresses can be constructed. Standard attributes mean that their syntax and semantics are defined in ISO/IEC 10021-2. In addition to standard attributes, and to cater for existing messaging systems, there are domain defined attributes whose syntax and semantics are defined by Management Domains.

Various forms of OR-addresses are defined, each serving their own purpose. These forms and their purpose are as follows:

Mnemonic OR-Address: Provides a user friendly means of identifying users in the absence of a directory. It is also used for identifying a distribution list.

Terminal OR-Address: Provides a means of identifying users with terminals belonging to various networks.

Numeric OR-Address: Provides a means of identifying users by means of numeric keypads.

Postal OR-Address: Provides a means of identifying originators and recipients of physical messages.

13 MHS Use of Directory

13.1 Introduction

The Directory defined by ISO/IEC 9594 provides capabilities useful in the use and provision of a variety of telecommunication services. This clause describes how a directory can be used in message handling. Details can be found in other parts of ISO/IEC 10021.

The directory capabilities used in message handling fall into the following four categories:

a) **User-friendly naming**: The originator or recipient of a message can be identified by means of his directory name, rather than his machine oriented OR-address. At any time MHS can obtain the latter from the former by consulting the directory.

b) **Distribution lists (DLs)**: A group whose membership is stored in the directory can be used as a DL. The originator simply supplies the name of the list. At the DL's expansion point MHS can obtain the directory names (and then the OR-addresses) of the individual recipients by consulting the directory.

c) **Recipient UA capabilities**: MHS capabilities of a recipient (or originator) can be stored in his directory entry. At any time MHS can obtain (and then act upon) those capabilities by consulting the directory.

d) **Authentication**: Before two MHS functional entities (two MTAs, or a UA and an MTA) communicate with one another, each establishes the identity of the other. This can be done by using authentication capabilities of MHS based on information stored in the directory.

Besides the above, one user can directly access the directory, for example, to determine the OR-address or MHS capabilities of another. The recipient's directory name is supplied to the directory, which returns the requested information.

13.2 Functional Model

Both UAs and MTAs can use the directory. A UA can present the directory with the directory name of the intended recipient, and obtain from the directory, the recipient's OR-address. The UA can then supply both the directory name and the OR-address to the MTS. Another UA can supply just the recipient's directory name to the MTS. The MTS would then itself ask the directory for the recipient's OR-address and add it to the envelope. The originating MTA normally carries out the name-to-OR-address look-up using access rights granted to the MTA.

A functional model depicting the above is shown in Figure 13.

13.3 Physical Configurations

Some possible physical configurations of the above functional model are shown in Figure 14. Where a Directory User Agent (DUA) and Directory System Agent (DSA) reside in physically separate systems, a standard directory protocol, defined in ISO/IEC 9594, governs their interactions. It will often be desirable to physically co-locate a UA or MTA with a DUA/DSA. However, other physical configurations are also possible.

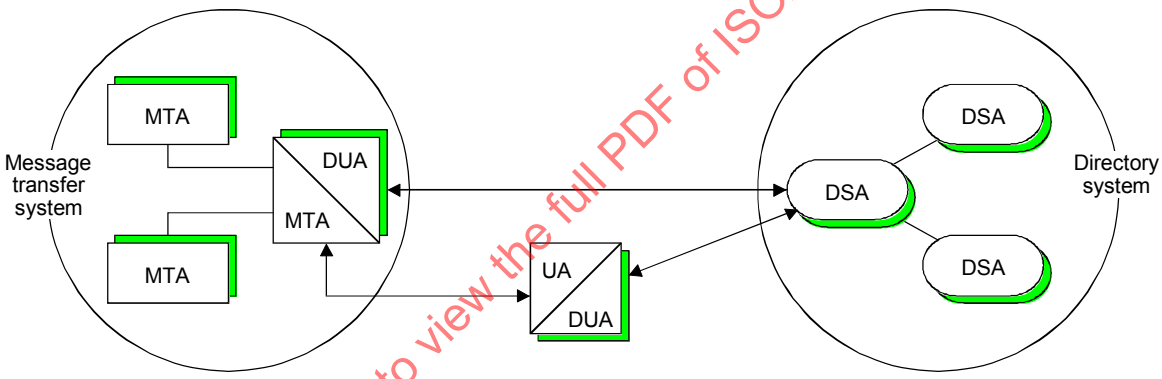


Figure 13 – Functional Model of MHS-Directory Interworking

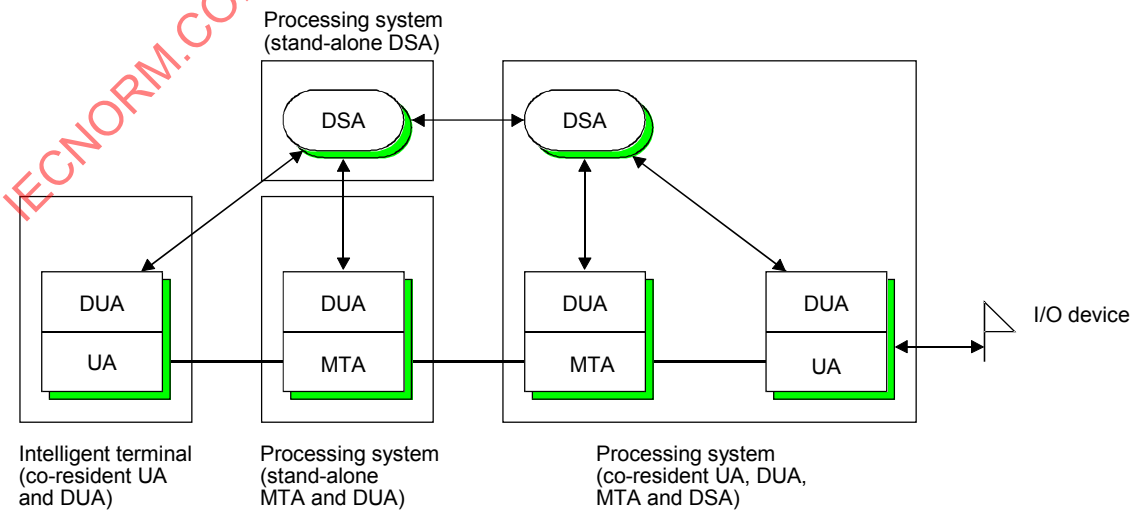


Figure 14 – Physical Configurations for MHS-Directory Interworking

14 Distribution Lists in MHS

14.1 Introduction

The ability to make use of a Distribution List (DL) is an optional capability of MHS provided through the MT Service. DL Expansion allows a sender to have a message transmitted to a group of recipients, by naming the group instead of having to enumerate each of the final recipients.

14.2 Properties of a DL

The properties of a DL can be described as follows:

DL Members: Users and other DLs that will receive messages addressed to the DL.

DL Submit Permission: A list of users and other DLs which are allowed to make use of the DL to send messages to the DL's members.

DL Expansion Point: Each DL has one or more OR-addresses, each of which unambiguously identifies the DL. When a message is addressed to a DL, the OR-address is used to locate an expansion point, which is a domain or MTA where the names of the members of the DL are added to the recipient list. The message is transported to the expansion point before expansion, as shown in Figure 15. There may be more than one MTA capable of acting as the DL expansion point for a particular DL, especially if the Directory is used to store the membership of the DL.

DL Owner: A user who is responsible for the management of a DL.

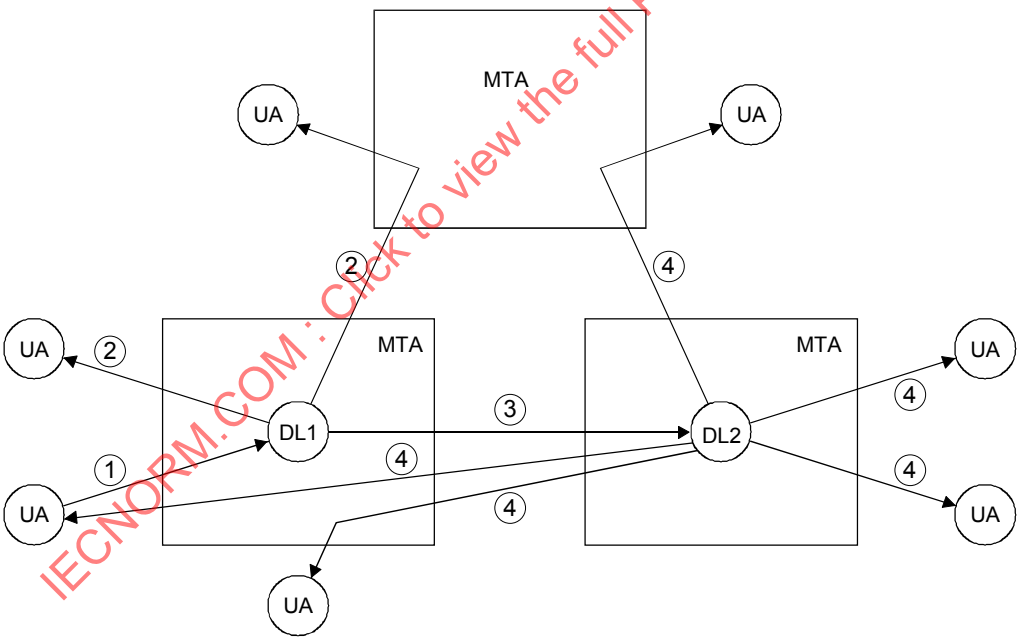


Figure 15 – Distribution List Expansion

14.3 Submission

Submission of a message to a DL is similar to the submission of a message to a user. The originator can include in the DL's OR-name, the directory name, the OR-address, or both (see clause 12 for details). The originator need not be aware that the OR-name used is that of a DL. The originator can, however, through use of the Element of Service, DL Expansion Prohibited, prohibit the MTS from expanding a message unknowingly addressed to a DL.

14.4 DL Use of a Directory

A directory may or may not be used to store information about the properties of a DL. Among the information that can be stored are the following: DL members, DL owner, DL submit permission and the DL expansion point.

14.5 DL Expansion

At the expansion point, the MTA responsible for expanding the DL will:

a) Look up the information about the DL, e.g. in the directory, using access rights granted to the MTA.
NOTE – Since this is done by the MTA at the expansion point, support of DLs in MHS does not require a globally interconnected directory.

b) Verify whether expansion is allowed by checking the identity of the sender against the DL's submit permission.

c) If expansion is allowed, add the members of the DL (except any exempted recipients) to the list of recipients of the message and transmit the message to them.

14.6 Nesting

A member of a DL can be another DL as shown in Figure 15. In this case the message is forwarded from the expansion point of the parent DL for further expansion. Thus during each expansion, only the members of a single DL are added to the message.

During expansion of a nested DL, the identity of the parent DL (e.g. DL1 in Figure 15) rather than that of the message originator, is compared against the submit permission of the member DL (e.g. DL2 in Figure 15).

NOTE – DL structures can be defined which reference a particular nested DL more than once at different levels of the nesting. Submission to such a parent DL can cause a recipient to receive multiple copies of the same message. The same result can occur if a message is addressed to multiple DLs which contain a common member. Correlation of such copies can be done at the recipient's UA, and/or in the MS.

14.7 Recursion Control

If a certain DL is directly or indirectly a member of itself (a situation which can validly arise), or when DLs are combined with redirection, then a message might get back to the same list and potentially circulate infinitely. This is detected by the MTS and prevented from occurring.

14.8 Delivery

On delivery of the message, the recipient will find out that he received the message as a member of a DL, and through which DL, or chain of DLs he received the message.

14.9 Routing Loop Control

A message can be originated in one domain/MTA, expanded in a second domain/MTA, and then sent back to a DL member in the first domain/MTA. The MTS will not treat this as a routing loop error.

14.10 Notifications

Delivery and Non-delivery Notifications can be generated both at the DL-expansion point (e.g. if submit permission is denied), and at delivery to the ultimate recipient.

When a message coming from a DL generates a notification, this notification is sent to the DL from which the message came. The DL will then, depending on the policy of the list, forward the notification to the owner of the list, to the DL or originator from which it received the message, or both, as shown in Figure 16.

NOTE – When notifications are sent to the originator after DL expansion, the originator can receive many Delivery/Non-delivery Notifications for one originator specified recipient (the DL itself). The originator can even receive more than one notification from an ultimate recipient, if that recipient received the message more than once via different lists.

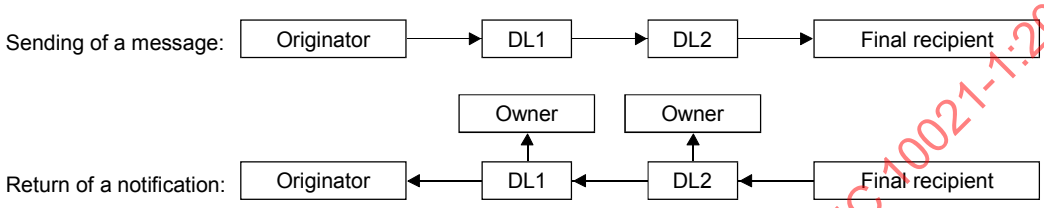


Figure 16 – DL Notifications

14.11 DL Handling Policy

An MTA may or may not provide different policies on DL handling. Such policies will control whether notifications generated at delivery to DL members should be propagated back through the previous DL, or to the originator if no such previous DL, and/or to the list owner. If the policy is such that notifications are to be sent only to the list owner, then the originator will receive notifications if requested, only during expansion of that DL. In order to accomplish this restriction, the MTS will, while performing the expansion, reset the notification requests according to the policy for the list.

15 Security Capabilities of MHS

15.1 Introduction

The distributed nature of MHS makes it desirable that mechanisms are available to protect against various security threats that can arise. The nature of these threats and the capabilities to counter them are highlighted below.

15.2 MHS Security Threats

15.2.1 Access Threats

Invalid user access into MHS is one of the prime security threats to the system. If invalid users can be prevented from using the system, then the subsequent security threat to the system is greatly reduced.

15.2.2 Inter-Message Threats

Inter-message threats arise from unauthorized agents who are external to the message communication, and can manifest themselves in the following ways:

Masquerade: A user who does not have proof of whom he is talking to can be easily misled by an impostor into revealing sensitive information.

Message Modification: A genuine message which has been modified by an unauthorized agent while it was transferred through the system can mislead the message recipient.

Replay: Messages whose originators and contents are genuine can be monitored by an unauthorized agent and could be recorded to be replayed to the message's intended recipient at a later date. This could be done in order to either extract more information from the intended recipient or to confuse him.

Traffic Analysis: Analysis of message traffic between MH users can reveal to an eavesdropper how much data (if any) is being sent between users and how often. Even if the eavesdropper cannot determine the actual contents of the messages, he can still deduce a certain amount of information from the rate of traffic flow (e.g. continuous, burst, sporadic or none).

15.2.3 Intra-Message Threats

Intra-message threats are those performed by the actual message communication participants themselves, and can manifest themselves in the following ways:

Repudiation of Messages: One of the actual communication participants can deny involvement in the communication. This could have serious implications if financial transactions were being performed via MHS.

Security Level Violation: If a management domain within MHS employs different security clearance levels (e.g. public, personal, private and company confidential), then users must be prevented from sending or receiving any messages for which they have an inadequate security clearance level if the Management Domain's security is not to be compromised.

15.2.4 Data Store Threats

An MHS has a number of data stores within it that must be protected from the following threats:

Modification of Routing Information: Unauthorized modification of the directory's contents could lead to messages being mis-routed or even lost while unauthorized modification to the deferred delivery data store or the hold for delivery data store could mislead or confuse the intended recipient.

Preplay: An unauthorized agent could make a copy of a deferred delivery message and send this copy to the intended recipient while the original was still being held for delivery in the MTA. This could fool the message recipient into replying to the message originator before the originator was expecting a reply or simply mislead or confuse the original intended message recipient.

15.3 Security Model

Security features can be provided by extending the capabilities of the components in the Message Handling System to include various security mechanisms.

There are two aspects to security in message handling: Secure Access Management and Administration, and Secure Messaging.

15.3.1 Secure Access Management and Administration

The capabilities in this section cover the establishment of an authenticated association between adjacent components, and the setting up of security parameters for that association. This can be applied to any pair of components in the Message Handling System: UA/MTA, MTA/MTA, MS/MTA, etc.

15.3.2 Secure Messaging

The capabilities in this section cover the application of security features to protect messages in the Message Handling System in accordance with a defined security policy. This includes Elements of Service enabling various components to verify the origin of messages and the integrity of their content, and Elements of Service to prevent unauthorized disclosure of the message content.

The capabilities in this section cover the application of security features to protect messages directly submitted to the Message Transfer System by a User Agent, Message Store, or an Access Unit. They do not cover the application of security features to protect communication between users and the Message Handling System, or MH user-to-MH user communication (a large part of MH user-to-MH user communication is protected between two UAs). Thus they do not apply, for example, to communication between a remote user's terminal and its UA, or to communication between these users' terminal equipment and other users in the MHS.

Many of the secure messaging Elements of Service provide an originator-to-recipient capability, and require the use of User Agents with security capabilities. They do not require the use of a Message Transfer System with security features. (As an example, content confidentiality can be applied by enciphering the message content by the originator, and deciphering by the recipient, with various security parameters transferred within the message envelope. Such a message can be transferred by any MTS which can handle the format of the content (unformatted octets), and transparently handle the security fields in the envelope.)

Some of the secure messaging Elements of Service involve an interaction with the Message Transfer System, and require the use of Message Transfer Agents with security capabilities. (As an example, Non-repudiation of Submission requires the MTA, to which the message is submitted, to contain mechanisms to generate a proof of submission field.)

Some of the secure messaging Elements of Service apply to the MS as well as UAs and MTAs, such as Message Security Labelling. In general, however, the MS is transparent to security features that apply between the originators' and the recipient's UAs.

The scope of the secure messaging Elements of Service is given in Table 2. This describes the Elements of Service in terms of which MHS component is the "provider" or which is the "user" of the security service. For example, Probe Origin Authentication is provided by the originating UA, and can be used by the MTAs through which the probe passes.

This part of ISO/IEC 10021 describes the use of security services by the UA, MS and the MTA. How these features are applied to Access Units may be the subject of future standardisation.

15.4 MHS Security Capabilities

The Elements of Service describing the security features of MHS are defined in Annex B, and classified in clause 19. An overview of these capabilities is as follows:

Message Origin Authentication: Enables the recipient, or any MTA through which the message passes, to authenticate the identity of the originator of a message.

Report Origin Authentication: Allows the originator to authenticate the origin of a delivery/non-delivery report.

Probe Origin Authentication: Enables any MTA through which the probe passes to authenticate the origin of the probe.

Proof of Delivery: Enables the originator of a message to authenticate the delivered message and its content, and the identity of the recipient(s).

Proof of Submission: Enables the originator of a message to authenticate that the message was submitted to the MTS for delivery to the originally specified recipient(s).

Secure Access Management: Provides for authentication between adjacent components, and the setting up of the security context.

Content Integrity: Enables the recipient to verify that the original content of a message has not been modified.

Content Confidentiality: Prevents the unauthorized disclosure of the content of a message to a party other than the intended recipient.

Message Flow Confidentiality: Allows the originator of a message to conceal the message flow through MHS.

Message Sequence Integrity: Allows the originator to provide to a recipient proof that the sequence of messages has been preserved.

Non-repudiation of Origin: Provides the recipient(s) of a message with proof of origin of the message and its content which will protect against any attempt by the originator to falsely deny sending the message or its content.

Non-repudiation of Delivery: Provides the originator of a message with proof of delivery of the message which will protect against any attempt by the recipient(s) to falsely deny receiving the message of its content.

Non-repudiation of Submission: Provides the originator of a message with proof of submission of the message, which will protect against any attempt by the MTS to falsely deny that the message was submitted for delivery to the originally specified recipient(s).

Message Security Labelling: Provides a capability to categorize a message, indicating its sensitivity, which determines the handling of a message in line with the security policy in force.

Table 2 – Provision and Use of Secure Messaging Elements of Service by MHS Components

Elements of Service	Originating MTS User	MTS	Recipient MTS User
Message Origin Authentication	P	U	U
Report Origin Authentication	U	P	–
Probe Origin Authentication	P	U	–
Proof of Delivery	U	–	P
Proof of Submission	U	P	–
Secure Access Management	P	U	P
Content Integrity	P	–	U
Content Confidentiality	P	–	U
Message Flow Confidentiality	P	–	–
Message Sequence Integrity	P	–	U
Non-repudiation of Origin	P	–	U
Non-repudiation of Submission	U	P	–
Non-repudiation of Delivery	U	–	P
Message Security Labelling	P	U	U
P The MHS component is a provider of the service U The MHS component is a user of the service			

15.5 Security Management

Aspects of an asymmetric key management scheme to support the above features are provided by the Directory System Authentication Framework, described in ISO/IEC 9594-8. The directory stores certified copies of public keys for MH users which can be used to provide authentication and to facilitate key exchange for use in data confidentiality and data integrity mechanisms. The certificates can be read from the Directory using the Directory Access Protocol described in ISO/IEC 9594-5.

Other types of key management schemes, including symmetric encryption, to support the security features may be the subject of future standardisation.

15.6 MHS Security Dependencies

If, as a result of using MHS Security capabilities, there are any dependencies, consequences or restrictions on other MHS capabilities (e.g. on Distribution Lists or Conversion), then these shall be defined by the security policy. For example, a security policy may specify that the Conversion Prohibition Element of Service shall always be selected.

An abstract security model for Message Transfer is described in clause 10 of ISO/IEC 10021-2. In particular, 10.1 of ISO/IEC 10021-2 describes the concept of security policy.

15.7 IPM Security

The Elements of Service describing the additional security features of IPMS are defined in Annex B, and classified in clause 19. An overview of these capabilities is as follows:

Request for Non-repudiation of Content Received	Enables the originator of an IP-message to request that the recipient of the IP-message provides irrevocable proof that the recipient received and verified the integrity of the IP-message content. This Element of Service provides only an indication of the originator's request. Fulfilment of the request requires support of the Non-repudiation of Content Received Element of Service.
Non-repudiation of Content Received	Provides the originator of an IP-message with irrevocable proof that the recipient validated the security features of the IP-message. This provides a proof with non-repudiation properties of the authenticity and integrity of the contents of the IP-message as it was received by the recipient. The recipient is required to fulfil the request for this Element of Service only when the UA is subject to a security policy which mandates the support of this Element of Service.
Request for Non-repudiation of IP-notification	Enables the originator of an IP-message to request that the recipient of the IP-message provides irrevocable proof that the recipient received the IP-message and the recipient of the IP-message originated the IP-notification. This Element of Service provides only an indication of the originator's request. Fulfilment of the request requires support of the Non-repudiation of IP-notification Element of Service.
Non-repudiation of IP-notification	Provides the originator of an IP-message with irrevocable proof that the IP-message was received by the recipient and that the recipient originated the resulting IP-notification. This provides a signed receipt of the IP-message identifier which has non-repudiation properties. The recipient is required to fulfil the request for this Element of Service only when the UA is subject to a security policy which mandates the support of this element of service.
Request for Proof of Content Received	Enables the originator of an IP-message to request that the recipient of the IP-message provides proof that the recipient received and verified the integrity of the IP-message contents. This Element of Service provides only an indication of the originator's request. Fulfilment of the request requires support of the Proof of Content Received Element of Service.
Proof of Content Received	Provides the originator of an IP-message with proof that the recipient validated the security features of the IP-message. This Element of Service provides proof of the authenticity and integrity of the contents of the IP-message as it was received by the recipient. The recipient is required to fulfil the request for this Element of Service only when the UA is subject to a security policy which mandates the support of this Element of Service.
Request for Proof of IP-notification	Enables the originator of an IP-message to request that the recipient of the IP-message provides proof that the recipient received the IP-message and the recipient of the IP-message originated the IP-notification. This Element of Service provides only an indication of the originator's request. Fulfilment of the request requires support of the Proof of IP-notification Element of Service.
Proof of IP-notification	Provides the originator of an IP-message with proof that the IP-message was received by the recipient and that the recipient originated the resulting IP-notification. This provides a signed receipt of the IP-message identifier. The recipient is required to fulfil the request for this Element of Service only when the UA is subject to a security policy which mandates the support of this Element of Service.

The application of security features between the IPM-UA and the MHS user, such as user authentication and local access control, is a local matter. Information required to implement local access control may be conveyed between the originator and recipient IPM-UAs using the Message Security Labelling Element of Service. The syntax and semantics of private and local access control information may be defined by registration of security policies and security categories.

The above IPM-UA security features use the MHS security capabilities defined in ITU-T Rec. X.411 | ISO/IEC 10021-4 provided by the user of the MTS. They do not require any extensions to the MTS defined in ITU-T Rec. X.411 | ISO/IEC 10021-4. IPM-UAs which support the above security features are required to support the related protocol extensions and associated procedures defined in ITU-T Rec. X.420 | ISO/IEC 10021-7. The IPM-UA security features use the MTS-User security mechanisms defined in ITU-T Rec. X.411 | ISO/IEC 10021-4 such as Content-integrity-check, Message-origin-authentication-check, and Message-token. The IPM-UA security features do not define any additional security mechanisms.

NOTE – In case of the use of a notarizing function, non-repudiation can be provided implicitly, and is not reflected in any specific protocol elements.

Table 3 – Provision and use of additional secure messaging Elements of Service by IPM-UAs

Elements of Service	IP-message Originator	MTS	IP-message Recipient
Request for Non-repudiation of Content Received	Requester	–	User
Non-repudiation of Content Received	User	–	Provider
Request for Non-repudiation of IP-notification	Requester	–	User
Non-repudiation of IP-notification	User	–	Provider
Request for Proof of Content Received	Requester	–	User
Proof of Content Received	User	–	Provider
Request for Proof of IP-notification	Requester	–	User
Proof of IP-notification	User	–	Provider

16 Conversion in MHS

The MTS provides conversion functions to allow users to input messages in one or more encoded formats, called encoded information types (EITs) and have them delivered in other EITs to cater to users with various UA capabilities and terminal types. This capability is inherent in the MTS and increases the possibility of delivery by tailoring the message to the recipient's terminal capabilities. The EITs standardized in MHS are listed in ISO/IEC 10021-4. Conversions and the use of the Elements of Service relating to conversion are available for EITs not defined in ISO/IEC 10021-4, but supported by certain domains, either bilaterally between these domains or within a domain itself.

MH users have some control over the conversion process through various Elements of Service as described in Annex B. These include the ability for a user to explicitly request the conversion required or as a default to let the MTS determine the need for conversion, and the type of conversion performed. Users also have the ability to request that conversion not be performed or that conversion not be performed if loss of information will result. When the MTS performs conversion on a message, it informs the UA to whom the message is delivered that conversion took place and what the original EITs were.

The conversion process for IP-messages can be performed on body parts of specific types if they are present in a message. The general aspects of conversion and the specific conversion rules for conversion between different EITs are detailed in CCITT Recommendation X.408.

CCITT Recommendation X.408 deals with conversion including the following: IA5 Text, G3Fax, G4 Class1, and Videotex.

17 *Clause 17 of the corresponding ITU-T Recommendation is not part of this International Standard*

18 Elements of Service – Purpose

Elements of Service are particular features, functions, or capabilities of MHS. All the Elements of Service applicable for MHS are defined in Annex B, where they are listed in alphabetical order with a corresponding reference number. The realization of these Elements of Service in MHS are described in other parts of ISO/IEC 10021.

Elements of Service are associated with the various services provided in MHS. There are Elements of Service for the Message Transfer Service which provide for a basic capability for sending and receiving messages between UAs. There are Elements of Service for the Interpersonal Messaging Service which provide for the sending and receiving of messages between a particular class of UAs called IPM UAs. There are Elements of Service for the Physical Delivery Service, enabling MH users to send messages and have them delivered in a physical medium to non-MH users. There are Elements of Service specifically available for the use of Message Stores.

The Elements of Service for the IPM Service include those available for the MT Service, the PD Service and the Message Store as well as specific ones applicable to the IPM Service.

Table 4 lists all the Elements of Service available in MHS, shows what services they are associated with of the presently defined services, MT Service, IPM Service, PD Service, and MS Service, and gives the corresponding reference number to the definition in Annex B. Elements of Service relevant to the IPM Message Store are marked on both the IPM and MS columns.

Table 4 – MHS elements of service

Elements of Service	MT	IPM	PD	MS	Annex B Reference
Access Management	X				B.1
Additional Physical Rendition			X		B.2
Alternate Recipient Allowed	X				B.3
Alternate Recipient Assignment	X				B.4
Authorization Time Indication		X			B.5
Authorizing Users Indication		X			B.6
Auto-acknowledgment of IP-messages		X		X	B.7
Auto-action Log				X	B.8
Auto-advise		X		X	B.9
Auto-assignment of Annotations				X	B.10
Auto-assignment of Group Names				X	B.11
Auto-assignment of Storage Period				X	B.12
Auto-correlation of IP-messages		X		X	B.13
Auto-correlation of IP-notifications		X		X	B.14
Auto-correlation of Reports				X	B.15
Auto-deletion after Storage Period				X	B.16
Auto-discarding of IP-messages		X		X	B.17
Auto-forwarded Indication		X			B.18
Auto-forwarding of IP-messages		X		X	B.19
Auto-submitted Indication		X			B.20
Basic Physical Rendition			X		B.21
Blind Copy Recipient Indication		X			B.22

Table 4 – MHS elements of service (*continued*)

Elements of Service	MT	IPM	PD	MS	Annex B Reference
Body Part Authentication and Integrity		X			B.23
Body Part Encryption		X			B.24
Circulation List Recipients Indication		X			B.25
Content Confidentiality	X				B.26
Content Integrity	X				B.27
Content Type Indication	X				B.28
Conversion Prohibition	X				B.29
Conversion Prohibition in Case of Loss of Information	X				B.30
Converted Indication	X				B.31
Counter Collection			X		B.32
Counter Collection with Advice			X		B.33
Cover Page Suppression	X				B.34
Cross-referencing Indication		X			B.35
Deferred Delivery	X				B.36
Deferred Delivery Cancellation	X				B.37
Delivery Log				X	B.38
Delivery Notification	X				B.39
Delivery Time Stamp Indication	X				B.40
Delivery via Bureaufax Service			X		B.41
Designation of Recipient by Directory Name	X				B.42
Disclosure of Other Recipients	X				B.43
Distribution Codes Indication		X			B.44
DL Exempted Recipients	X				B.45
DL Expansion History Indication	X				B.46
DL Expansion Prohibited	X				B.47
EMS (Express Mail Service)			X		B.48
Expiry Date Indication		X			B.49
Explicit Conversion	X				B.50
Forwarded IP-message Indication		X			B.51
Grade of Delivery Selection	X				B.52
Hold for Delivery	X				B.53
Implicit Conversion	X				B.54
Importance Indication		X			B.55
Incomplete Copy Indication		X			B.56
Information Category Indication		X			B.57
IP-message Action Status		X		X	B.58
IP-message Identification		X			B.59
IP-message Security Labelling		X			B.60
Language Indication		X			B.61
Latest Delivery Designation	X				B.62
Manual Handling Instructions Indication		X			B.63

Table 4 – MHS elements of service (*continued*)

Elements of Service	MT	IPM	PD	MS	Annex B Reference
Message Flow Confidentiality	X				B.64
Message Identification	X				B.65
Message Origin Authentication	X				B.66
Message Security Labelling	X				B.67
Message Sequence Integrity	X				B.68
MS Register				X	B.69
Multi-destination Delivery	X				B.70
Multi-part Body		X			B.71
Non-delivery Notification	X				B.72
Non-receipt Notification Request Indication		X			B.73
Non-repudiation of Content Received		X			B.74
Non-repudiation of Delivery	X				B.75
Non-repudiation of IP-Notification		X			B.76
Non-repudiation of Origin	X				B.77
Non-repudiation of Submission	X				B.78
Obsoleting Indication		X			B.79
Ordinary Mail			X		B.80
Original Encoded Information Types Indication	X				B.81
Originator Indication		X			B.82
Originator Reference Indication		X			B.83
Originator Requested Alternate Recipient	X				B.84
Physical Delivery Notification by MHS			X		B.85
Physical Delivery Notification by PDS			X		B.86
Physical Forwarding Allowed			X		B.87
Physical Forwarding Prohibited			X		B.88
Precedence Indication		X			B.89
Prevention of Non-delivery Notification	X				B.90
Primary and Copy Recipients Indication		X			B.91
Probe		X			B.92
Probe Origin Authentication	X				B.93
Proof of Content Received		X			B.94
Proof of Delivery	X				B.95
Proof of IP-notification		X			B.96
Proof of Submission	X				B.97
Receipt Notification Request Indication		X			B.98
Redirection Disallowed by Originator	X				B.99
Redirection of Incoming Messages	X				B.100
Registered Mail			X		B.101
Registered Mail to Addressee in Person			X		B.102
Reply Request Indication		X			B.103
Replying IP-message Indication		X			B.104
Report Origin Authentication	X				B.105

Table 4 – MHS elements of service (*concluded*)

Elements of Service	MT	IPM	PD	MS	Annex B Reference
Request for Forwarding Address			X		B.106
Request for Non-repudiation Of Content Received		X			B.107
Request for Non-repudiation Of IP-Notification		X			B.108
Request for Proof of Content Received		X			B.109
Request for Proof of IP-notification		X			B.110
Requested Preferred Delivery Method	X				B.111
Restricted Delivery	X				B.112
Return of Content	X				B.113
Secure Access Management	X				B.114
Sensitivity Indication		X			B.115
Special Delivery			X		B.116
Storage of Draft Messages				X	B.117
Storage on Submission				X	B.118
Storage Period Assignment				X	B.119
Stored Message Alert				X	B.120
Stored Message Annotation				X	B.121
Stored Message Deletion				X	B.122
Stored Message Fetching				X	B.123
Stored Message Grouping				X	B.124
Stored Message Listing				X	B.125
Stored Message Summary				X	B.126
Subject Indication		X			B.127
Submission Log				X	B.128
Submission of IP-messages Incorporating Stored Messages		X		X	B.129
Submission Time Stamp Indication	X				B.130
Typed Body		X			B.131
Undeliverable Mail with Return of Physical Message			X		B.132
Use of Distribution List	X				B.133
User/UA Capabilities Registration	X				B.134

19 Elements of service – Classification

19.1 Purpose of Classification

The Elements of Service of MHS are classified either as belonging to a basic (also called base for PD and MS) service, or as optional user facilities. Elements of Service belonging to a basic service are inherently part of that service; they constitute the basic service and are always provided and available for use of that service.

Other Elements of Service, called optional user facilities, can be selected by the subscriber or user, either on a per-message basis, or for an agreed contractual period of time. Each optional user facility is classified as either essential or additional. Essential (E) optional user facilities are to be made available to all MH users. Additional (A) optional user facilities can be made available for national use, and for international use on the basis of bilateral agreement.

19.2 Basic Message Transfer Service

The basic MT service enables a UA to submit and to have messages delivered to it. If a message cannot be delivered, the originating UA is so informed through a Non-delivery Notification. Each message is uniquely and unambiguously identified. To facilitate meaningful communication, a UA can specify the encoded information type(s) that can be contained in messages which are delivered to it. The content type and original encoded information type(s) of a message and an indication of any conversions that have been performed, and the resulting encoded information type(s), are supplied with each delivered message. In addition, the submission time and delivery time are supplied with each message. The MT Elements of Service belonging to the basic MT Service are listed in Table 5.

Table 5 – Elements of Service Belonging to The Basic MT Service

Elements of Service	Annex B Reference
Access management	B.1
Content type indication	B.28
Converted indication	B.31
Delivery time stamp indication	B.40
Message identification	B.65
Non-delivery notification	B.72
Original encoded information types indication	B.81
Submission time stamp indication	B.130
User/UA capabilities registration	B.134

19.3 MT Service Optional User Facilities

Optional user facilities for the MT Service can be selected on a per-message basis, or for an agreed period of time. Each optional user facility is classified as either essential or additional as described in 19.1. Table 6 lists the Elements of Service comprising the optional user facilities of the MT Service with their classification and their availability (PM = per-message; CA = Contractual Agreement). Optional user facilities for the PD Service and the Message Store, while forming a part of the MT Service optional user facilities, are not listed in this table because they are subject to either a PDAU or an MS being supplied, and are given separate classifications in Tables 7 - 10.

A security policy will define when the security related MT Service Optional User Facilities are invoked.

Table 6 – MT Service Optional User Facilities

Elements of Service	Classification	Available	Annex B Reference
Alternate Recipient Allowed	E	PM	B.3
Alternate Recipient Assignment	A	CA	B.4
Content Confidentiality	A	PM	B.26
Content Integrity	A	PM	B.27
Conversion Prohibition	E	PM	B.29
Conversion Prohibition in Case of Loss of Information	A	PM	B.30
Cover Page Suppression	A	PM	B.34
Deferred Delivery	E	PM	B.36
Deferred Delivery Cancellation	E	PM	B.37
Delivery Notification	E	PM	B.39
Designation of Recipient by Directory Name	A	PM	B.42
Disclosure of Other Recipients	E	PM	B.43
DL-Exempted Recipients	A	PM	B.45
DL-Expansion History Indication	A	PM	B.46
DL-Expansion Prohibited	A	PM	B.47
Explicit Conversion	A	PM	B.50
Grade of Delivery Selection	E	PM	B.52
Hold for Delivery	A	CA	B.53
Implicit Conversion	A	CA	B.54
Latest Delivery Designation	A	PM	B.62
Message Flow Confidentiality	A	PM	B.64
Message Origin Authentication	A	PM	B.66
Message Security Labelling	A	PM	B.67
Message Sequence Integrity	A	PM	B.68
Multi-Destination Delivery	E	PM	B.70
Non-Repudiation of Delivery	A	PM	B.75
Non-Repudiation of Origin	A	PM	B.77
Non-Repudiation of Submission	A	PM	B.78
Originator Requested Alternate Recipient	A	PM	B.84
Prevention of Non-delivery Notification	A	PM	B.90
Probe	A	PM	B.92
Probe Origin Authentication	A	PM	B.93
Proof of Delivery	A	PM	B.95
Proof of Submission	A	PM	B.97
Redirection Disallowed by Originator	A	PM	B.99
Redirection of Incoming Messages	A	PM	B.100
Report Origin Authentication	A	PM	B.105
Requested Preferred Delivery Method	A *	PM	B.111
Restricted Delivery	A	PM	B.112
Return of Content	A	PM	B.113
Secure Access Management	A	CA	B.114
Use of Distribution List	A	PM	B.133

A* Does not imply the provision of all delivery methods which may be requested.

19.4 Base MH/PD Service Intercommunication

The base MH/PD Service intercommunication can be supplied, to enhance the MT Service, and enables messages to be delivered to recipients in a physical (typically hard copy) format via a Physical Delivery Service such as the Postal Service. This capability is applicable for use by any application making use of the MT Service. The MH/PD Elements of Service belonging to the base MH/PD Service intercommunication are available on a per-recipient basis and are listed in Table 7. When this intercommunication is provided, through a PDAU, all the Elements of Service shown in Table 7 shall be supported.

Table 7 – Elements of Service Belonging to the Base MH/PD Service Intercommunication

Elements of Service	Annex B Reference
Basic Physical Rendition	B.21
Ordinary Mail	B.80
Physical Forwarding Allowed	B.87
Undeliverable Mail with Return of Physical Message	B.132

19.5 Optional User Facilities for MH/PD Service Intercommunication

Base MH/PD Elements of Service (see 19.4) together with the optional user facilities listed below can be used together for the provision of the MH/PD Service intercommunication. This capability is applicable for use by any application making use of the enhanced MT Service. These optional user facilities can be selected on a per-recipient basis and are listed in Table 8.

Table 8 – Optional User Facilities for MH/PD Service Intercommunication

Elements of Service	Classification	Annex B Reference
Additional Physical Rendition	A	B.2
Counter Collection	E	B.32
Counter Collection with Advice	A	B.33
Delivery via Bureaufax Service	A	B.41
EMS (Express Mail Service)[1)]	E	B.48
Physical Delivery Notification by MHS	A	B.85
Physical Delivery Notification by PDS	A	B.86
Physical Forwarding Prohibited	A	B.88
Registered Mail	A	B.101
Registered Mail to Addressee in Person	A	B.102
Request for Forwarding Address	A	B.106
Special Delivery [1)]	E	B.116

[1)] At least one or the other shall be supported by the PDAU and the associated PDS.

19.6 Base Message Store

The Base Message Store is optionally available to provide for storage and management of incoming messages acting as an intermediary between a UA and an MTA. The MS is applicable for use in any application making use of the MT Service. The elements of service belonging to the Base Message Store are listed in Table 9. When an MS is provided, each Element of Service shown in Table 9 shall be supported for every type of message (delivered-message, submission-log, draft-messages etc.) stored in the MS to which that Element of Service is applicable.

Table 9 – Base Message Store

Elements of Service	Annex B Reference
MS Register	B.69
Stored Message Deletion	B.122
Stored Message Fetching	B.123
Stored Message Listing	B.125
Stored Message Summary	B.126

19.7 MS Optional User Facilities

Base MS Elements of Service (see 19.6) together with the optional user facilities can be used for enhanced use of a Message Store. The enhanced MS is applicable for use in any application making use of the MT Service. The Elements of Service comprising the MS Optional User Facilities are listed in Table 10.

Table 10 – MS Optional User Facilities

Elements of Service	Classification	Annex B Reference
Auto-action Log	A	B.8
Auto-assignment of Annotations	A	B.10
Auto-assignment of Group Names	A	B.11
Auto-assignment of Storage Period	A	B.12
Auto-correlation of Reports	A	B.15
Auto-deletion after Storage Period	A	B.16
Delivery Log	A	B.38
Storage of Draft Messages	A	B.117
Storage on Submission	A	B.118
Storage Period Assignment	A	B.119
Stored Message Alert	A	B.120
Stored Message Annotation	A	B.121
Stored Message Grouping	A	B.124
Submission Log	A	B.128

19.8 Basic Interpersonal Messaging Service

The basic IPM Service, which makes use of the MT Service, enables a user to send and receive IP-messages. A user prepares IP-messages with the assistance of his User Agent (UA). User Agents cooperate with each other to facilitate communication between their respective users. To send an IP-message, the originating user submits the message to his UA specifying the OR-name of the recipient who is to receive the IP-message. The IP-message, which has an identifier conveyed with it, is then sent by the originator's UA to the recipient's UA via the Message Transfer Service.

Following a successful delivery to the recipient's UA, the IP-message can be received by the recipient. To facilitate meaningful communication, a recipient can specify the encoded information type(s) contained in IP-messages that he will allow to be delivered to his UA. The original encoded information type(s) and an indication of any conversions that have been performed and the resulting encoded information type(s) are supplied with each delivered IP-message. In addition, the submission time and delivery time are supplied with each IP-message. Non-delivery Notification is provided with the basic service. The IPM Elements of Service belonging to the basic IPM Service are listed in Table 11.

Table 11 – Elements of Service Belonging To The Basic IPM service

Elements of Service	Annex B Reference
Access Management	B.1
Content Type Indication	B.28
Converted Indication	B.31
Delivery Time Stamp Indication	B.40
IP-message Identification	B.59
Message Identification	B.65
Non-delivery Notification	B.72
Original Encoded Information Types Indication	B.81
Submission Time Stamp Indication	B.130
Typed Body	B.131
User/UA Capabilities Registration	B.134

19.9 IPM Service Optional User Facilities

A set of the Elements of Service of the IPM Service are optional user facilities. The optional user facilities of the IPM Service, which can be selected on a per-message basis or for an agreed contractual period of time, are listed in Tables 12 and 13, respectively. Local user facilities can be usefully provided in conjunction with some of these user facilities.

The optional user facilities of the IPM Service that are selected on a per-message basis are classified for both origination and reception by UAs. If an MD offers these optional user facilities for origination by UAs, then a user is able to create and send IP-messages according to the procedures defined for the associated Element of Service. If an MD offers these optional user facilities for reception by UAs, MSs and AUs, then the receiving UA, MS and PDAU will be able to receive and recognize the indication associated with the corresponding Element of Service and to inform the user of the requested optional user facility. Each optional user facility is classified as additional (A) or essential (E) for UAs from these two perspectives.

A security policy will define and determine when the security related IPM Service Optional User Facilities are invoked.

Table 12 – IPM Optional User Facilities Selectable on a Per-message Basis

Elements of Service	Origination	Reception	Annex B Reference
Additional Physical Rendition	A	A	B.2
Alternate Recipient Allowed	A	A	B.3
Authorization Time Indication	A	A	B.5
Authorizing Users Indication	A	E	B.6
Auto-Forwarded Indication	A	E	B.18
Auto-submitted Indication	A	E	B.20
Basic Physical Rendition	A	E*	B.21
Blind Copy Recipient Indication	A	E	B.22
Body Part Authentication and Integrity	A	A	B.23
Body Part Encryption	A	E	B.24
Circulation List Recipients Indication	A	A	B.25
Content Confidentiality	A	A	B.26
Content Integrity	A	A	B.27

Table 12 – IPM Optional User Facilities Selectable on a Per-message Basis (*continued*)

Elements of Service	Origination	Reception	Annex B Reference
Conversion Prohibition	E	E	B.29
Conversion Prohibition in Case of Loss of Information	A	A	B.30
Counter Collection	A	E*	B.32
Counter Collection with Advice	A	A	B.33
Cover Page Suppression	A	A	B.34
Cross-referencing Indication	A	E	B.35
Deferred Delivery	E	N/A	B.36
Deferred Delivery Cancellation	A	N/A	B.37
Delivery Notification	E	N/A	B.39
Delivery via Bureaufax Service	A	A	B.41
Designation of Recipient by Directory Name	A	N/A	B.42
Disclosure of Other Recipients	A	E	B.43
Distribution Codes Indication	A	A	B.44
DL-exempted Recipients	A	A	B.45
DL-expansion History Indication	N/A	E	B.46
DL-expansion Prohibited	A	N/A	B.47
EMS (Express Mail Service) (Note)	A	E*	B.48
Expiry Date Indication	A	E	B.49
Explicit Conversion	A	N/A	B.50
Forwarded IP-message Indication	A	E	B.51
Grade of Delivery Selection	E	E	B.52
Importance Indication	A	E	B.55
Incomplete Copy Indication	A	A	B.56
Information Category Indication	A	A	B.57
IP-message Security Labelling	A	A	B.60
Language Indication	A	A	B.61
Latest Delivery Designation	A	N/A	B.62
Manual Handling Instructions Indication	A	A	B.63
Message Flow Confidentiality	A	N/A	B.64
Message Origin Authentication	A	A	B.66
Message Security Labelling	A	A	B.67
Message Sequence Integrity	A	A	B.68
Multi-destination Delivery	E	N/A	B.70
Multi-part Body	A	E	B.71
Non-receipt Notification Request Indication	A	E	B.73
Non-repudiation of Content Received	A	A	B.74
Non-repudiation of Delivery	A	A	B.75
Non-repudiation of IP-notification	A	A	B.76
Non-repudiation of Origin	A	A	B.77
Non-repudiation of Submission	A	N/A	B.78
Obsoleting Indication	A	E	B.79

Table 12 – IPM Optional User Facilities Selectable on a Per-message Basis (*continued*)

Elements of Service	Origination	Reception	Annex B Reference
Ordinary Mail	A	E*	B.80
Originator Indication	E	E	B.82
Originator Reference Indication	A	A	B.83
Originator Requested Alternate Recipient	A	N/A	B.84
Physical Delivery Notification by MHS	A	A	B.85
Physical Delivery Notification by PDS	A	E*	B.86
Physical Forwarding Allowed	A	E*	B.87
Physical Forwarding Prohibited	A	E*	B.88
Precedence Indication	A	A	B.89
Prevention of Non-delivery Notification	A	N/A	B.90
Primary and Copy Recipients Indication	E	E	B.91
Probe	A	N/A	B.92
Probe Origin Authentication	A	N/A	B.93
Proof of Content Received	A	A	B.94
Proof of Delivery	A	A	B.95
Proof of IP-notification	A	A	B.96
Proof of Submission	A	N/A	B.97
Receipt Notification Request Indication	A	A	B.98
Redirection Disallowed by Originator	A	N/A	B.99
Registered Mail	A	A	B.101
Registered Mail to Addressee in Person	A	A	B.102
Reply Request Indication	A	E	B.103
Replying IP-message Indication	E	E	B.104
Report Origin Authentication	A	A	B.105
Request for Forwarding Address	A	A	B.106
Request for Non-repudiation of Content Received	A	A	B.107
Request for Non-repudiation of IP-notification	A	A	B.108
Request for Proof of Content Received	A	A	B.109
Request for Proof of IP-notification	A	A	B.110
Requested Preferred Delivery Method	A	A	B.111
Return of Content	A	N/A	B.113
Sensitivity Indication	A	E	B.115
Special Delivery (Note)	A	E*	B.116
Storage of Draft Messages	N/A	A	B.117
Storage on Submission	N/A	A	B.118
Storage Period Assignment	N/A	A	B.119
Stored Message Annotation	N/A	A	B.121
Stored Message Deletion	N/A	E***	B.122
Stored Message Fetching	N/A	E***	B.123
Stored Message Grouping	N/A	A	B.124

Table 12 – IPM Optional User Facilities Selectable on a Per-message Basis (*concluded*)

Elements of Service	Origination	Reception	Annex B Reference
Stored Message Listing	N/A	E**	B.125
Stored Message Summary	N/A	E**	B.126
Subject Indication	E	E	B.127
Submission of IP-messages Incorporating Stored Messages	N/A	A	B.129
Undeliverable Mail with Return of Physical Message	A	E*	B.132
Use of Distribution List	A	N/A	B.133

E	Essential optional user facility has to be provided.
E*	Essential optional user facility only applying to PDAUs.
E**	Essential optional user facility applying to MSs. Additional optional user facility applying to UAs (which connect to MSs).
E***	Essential optional user facility applying to MSs and UAs.
A	Additional optional user facility can be provided.
N/A	Not applicable.

1) At least EMS or Special Delivery shall be supported by the PDAU and associated PDS.

NOTE – Bilateral agreement may be necessary in cases of reception by UA of elements of service classified as "A".

Table 13 – IPM Optional User Facilities Agreed for a Contractual Period of Time

Elements of Service	Classification	Annex B Reference
Alternate Recipient Assignment	A	B.4
Auto-Acknowledgment of IP-messages	A	B.7
Auto-action Log	A	B.8
Auto-advise	A	B.9
Auto-assignment of Annotations	A	B.10
Auto-assignment of Group Names	A	B.11
Auto-assignment of Storage Period	A	B.12
Auto-correlation of IP-messages	A	B.13
Auto-correlation of IP-notifications	A	B.14
Auto-correlation of Reports	A	B.15
Auto-deletion After Storage Period	A	B.16
Auto-discarding of IP-messages	A	B.17
Auto-forwarding of IP-messages	A	B.19
Delivery Log	A	B.38
Hold for Delivery	A	B.53
Implicit Conversion	A	B.54
IP-message Action Status	A	B.58
MS Register	A	B.69
Redirection of Incoming Messages	A	B.100
Restricted Delivery	A	B.112
Secure Access Management	A	B.114
Stored Message Alert	A	B.120
Submission Log	A	B.128

Annex A
(informative)

Glossary of Terms

NOTE – The explanations given are not necessarily definitions in the strict sense. See also the definitions in Annex B and those provided in the other parts of ISO/IEC 10021 (especially ISO/IEC 10021-2), where many entries are sourced. The terms have, depending on the source, varying levels of abstraction.

A.1 Access Unit (AU)

In the context of a message handling system, the functional object, a component of MHS, that links another communication system (e.g. a physical delivery system or the telex network) to the MTS and via which its patrons engage in message handling as indirect users.

In the context of Message Handling Services, the unit which enables users of one service to intercommunicate with Message Handling Services, such as the IPM Service.

A.2 Actual Recipient

In the context of message handling, a potential recipient for which delivery or affirmation takes place.

A.3 Administration

The organisation that operates an ADMD.

NOTE – In the context of international regulations, an Administration is a national body that administers regulated Telecommunications and/or Postal services. In many countries, there is a separation of regulatory and operational bodies and an ITU Administration is not necessarily an operator of an ADMD service.

A.4 Administration Domain Name

In the context of message handling, a standard attribute of a name form that identifies an ADMD relative to the country denoted by a country name.

A.5 Administration Management Domain (ADMD)

A management domain that offers public message handling services to PRMDs and/or individual users. An ADMD has Administration responsibilities in order to ensure that its customers can communicate with any other MD attached to the global messaging backbone.

A.6 Alternate Recipient

In the context of message handling, a user or a distribution list to which a message or probe may be conveyed if, and only if, it cannot be conveyed to a particular preferred recipient. The Alternate Recipient may be specified by the originator (see B.84), by the recipient (see B.100), or by the recipient MD (see B.4).

A.7 Attribute

In the context of message handling, an information item, a component of an attribute list, that describes a user or distribution list and that can also locate it in relation to the physical or organizational structure of MHS (or the network underlying it).

A.8 Attribute List

In the context of message handling, a data structure, an ordered set of attributes, that constitutes an OR-address.

A.9 Attribute Type

An identifier that denotes a class of information (e.g. personal names). It is a part of an attribute.

A.10 Attribute Value

An instance of the class of information an attribute type denotes (e.g. a particular personal name). It is a part of an attribute.

A.11 Basic Service

In the context of message handling, the sum of features inherent in a service.

A.12 Body

Component of the content of an IP-message. Another component is the heading.

A.13 Body Part

Component of the body of an IP-message.

A.14 Common Name

In the context of message handling, a standard attribute of an OR-address form that identifies a user or distribution list relative to the entity denoted by another attribute (e.g. an organizational name).

A.15 Content

In the context of message handling, an information object, part of a message, that the MTS neither examines nor modifies, except for conversion, during its conveyance of the message.

A.16 Content Type

In the context of message handling, an identifier, on a message envelope, that identifies the type (i.e. syntax and semantics) of the message's content.

A.17 Conversion

In the context of message handling, a transmittal event in which an MTA transforms parts of a message's content from one encoded information type to another, or alters a probe so it appears that the described messages were so modified.

A.18 Country Name

In the context of message handling, a standard attribute of a name form that identifies a country (or, exceptionally, an International MD Registration Authority). A country name is a unique designation of a country for the purpose of sending and receiving messages.

NOTE – In the context of physical delivery, additional rules apply.

A.19 Delivery

In the context of message handling, a transmittal step in which an MTA conveys a message or report to the MS, UA or AU of a potential recipient of the message or of the originator of the report's subject message or probe.

A.20 Delivery Report

In the context of message handling, a report that acknowledges delivery, non-delivery, export, or affirmation of the subject message or probe, or distribution list expansion.

A.21 Direct Submission

In the context of message handling, a transmittal step in which the originator's UA or MS conveys a message or probe to an MTA.

A.22 Directory

A collection of open systems cooperating to provide directory services.

A.23 Directory Name

Name of an entry in a directory.

NOTE – In the context of message handling, the entry in the directory will enable the OR address to be retrieved for submission of a message.

A.24 Directory System Agent (DSA)

An OSI application process which is part of the directory, and whose role is to provide access to the directory information base to DUAs and/or other DSAs.

A.25 Directory User Agent (DUA)

An OSI application process which represents a user in accessing the directoy. Each DUA serves a single user so that the directory can control access to directory information on the basis of the DUA names. DUAs can also provide a range of local facilities to assist users to compose requests (queries) and interpret the responses.

A.26 Direct User

In the context of message handling, a user that engages in message handling by direct use of the MTS.

A.27 Distribution List (DL)

In the context of message handling, the functional object, a component of the message handling environment, that represents a pre-specified group of users and other distribution lists and that is a potential destination for the information objects an MHS conveys. Membership can contain OR-names identifying either users or other distribution lists.

A.28 Distribution List Expansion

In the context of message handling, a transmittal event in which an MTA resolves a distribution list, among a message's immediate recipients, to its members.

A.29 Distribution List Name

OR-name allocated to represent a collection of OR-addresses and directory names.

A.30 Domain

See Management Domain.

A.31 Domain Defined Attributes

Optional attributes of an OR-address allocated to names in the responsibility of a management domain.

A.32 Element Of Service

Functional unit for the purpose of segmenting and describing message handling features.

A.33 Encoded Information Type (EIT)

In the context of message handling, an identifier, on a message's envelope, that identifies one type of encoded information represented in the message's content. It identifies the medium and format (e.g. IA5 text, Group 3 facsimile) on an individual portion of the content.

A.34 Envelope

In the context of message handling, an information object, part of a message, whose composition varies from one transmittal step to another and that variously identifies the message originator and potential recipients, documents its past and directs its subsequent conveyance by the MTS, and characterizes its content.

A.35 Explicit Conversion

In the context of message handling, a conversion in which the originator selects both the initial and final encoded information types.

A.36 Extension Of Physical Delivery Address Components

Standard attribute of a postal OR-address as a means to give further information about the point of physical delivery in a postal address, e.g. the name of a hamlet, room and floor numbers in a large building.

A.37 Extension of Postal OR-Address Components

Standard attribute of a postal OR-address as a means to give further information to specify the addressee in a postal address, e.g. by organizational unit.

A.38 File Transfer Body Part

A body part for conveying the contents of a stored file, and other information associated with the file, from originator to recipient. The other information includes attributes which are typically stored along with the file content, information on the environment from which the transfer originated, and references to existing stored files or previous messages.

A.39 Formatted Postal OR-Address

Component of the content of a message. Another component is the body.

A.40 General Text Body Part

A body part that represents character text of a general nature, using 8-bit-encoding. It has parameters and data components. The parameter component identifies the character sets that are present in the data component. The data component comprises a single general string.

A.41 Heading

Component of an IP-message. Other components are the envelope and the body.

A.42 Immediate Recipient

In the context of message handling, one of the potential recipients assigned to a particular instance of a message or probe (e.g. an instance created by splitting).

A.43 Implicit Conversion

In the context of message handling, a conversion in which the MTA selects both the initial and final encoded information types.

A.44 Indirect Submission

In the context of message handling, a transmittal step in which an originator's UA conveys a message or probe to an MTA via an MS.

A.45 Indirect User

In the context of message handling, a user that engages in message handling by indirect use of MHS, i.e. through another communication system (e.g. a Physical Delivery System or the telex network) to which MHS is linked.

NOTE – Indirect users communicate via Access Units with direct users of MHS.

A.46 Intended Recipient

In the context of message handling, one of the users and distribution lists that the originator selects as a message's or probe's intended destination.

A.47 Intercommunication

In the context of message handling, a relationship between services, where one of the services is a Message Handling Service, enabling the user of the Message Handling Service to communicate with users of other services.

NOTE – Examples are the intercommunication between the IPM Service and the Telex Service, and the intercommunication between Message Handling Services and Physical Delivery Services.

A.48 Interpersonal Messaging Service

Messaging service between users belonging to the same management domain or to different management domains by means of message handling, based on the Message Transfer Service.

A.49 IP-message

The content of a message in the IPM Service.

A.50 Local Postal Attributes

Standard attributes of a postal OR-address as a means to distinguish between places with the same name (e.g. by state name, county name, or geographical attribute) in a postal address.

A.51 Management Domain (MD)

In the context of message handling, a set of messaging systems – at least one of which contains, or realizes, an MTA – that is managed by a single organization. It is a primary building block used in the organizational construction of MHS. It refers to an organizational area for the provision of services.

NOTE – A management domain may or may not necessarily be identical with a geographical area.

A.52 Management Domain Name

Unique designation of a management domain for the purpose of sending and receiving messages.

A.53 Members

In the context of message handling, the set of users and distribution lists implied by a distribution list name.

A.54 Message

An instance of the primary class of information object conveyed by means of message transfer, and comprising an envelope and content.

A.55 Message Handling (MH)

A distributed information processing task that integrates the intrinsically related subtasks of message transfer and message storage.

A.56 Message Handling Environment

The environment in which message handling takes place, comprising MHS, users, and distribution lists.

The sum of all components of message handling systems.

NOTE – Examples of components are:

- Message Transfer Agents;
- User Agents;
- Message Stores;
- Users.

A.57 Message Handling Service

Service provided by the means of Message Handling Systems.

NOTE 1 – Service may be provided through Administration Management Domains or Private Management Domains.

NOTE 2 – Examples of Message Handling Services are:

- Interpersonal Messaging Service (IPM service);
- Message Transfer Service (MT service).

A.58 Message Handling System (MHS)

The functional object, a component of the Message Handling Environment, that conveys information objects from one party to another.

A.59 Message Storage

The automatic storage for later retrieval of information objects conveyed by means of message transfer. It is one aspect of message handling.

A.60 Message Store (MS)

The functional object, a component of MHS, that provides a single direct user with capabilities for message storage.

A.61 Message Transfer (MT)

The non-real-time carriage of information objects between parties using computers as intermediaries. It is one aspect of message handling.

A.62 Message Transfer Agent (MTA)

A functional object, a component of the MTS, that actually conveys information objects to users and distribution lists.

A.63 Message Transfer Service

Service that deals with the submission, transfer and delivery of messages for other messaging services.

A.64 Message Transfer System (MTS)

The functional object consisting of one or more Message Transfer Agents which provides store-and-forward message transfer between User Agents, Message Stores and Access Units.

A.65 Messaging System

A computer system (possibly but not necessarily an open system) that contains, or realizes, one or more functional objects. It is a building block used in the physical construction of MHS.

A.66 Mnemonic OR-Address

An OR-address that mnemonicaly identifies a user or distribution list relative to the ADMD through which the user is accessed or the distribution list is expanded. It identifies an ADMD, and a user or distribution list relative to that ADMD.

A.67 Naming Authority

An authority responsible for the allocation of names.

A.68 Network Address

In the context of message handling, a standard attribute of an OR-address form that gives the network address of a terminal. It is comprising the numbering digits for network access points from an international numbering plan.

A.69 Non-delivery

In the context of message handling, a transmittal event in which an MTA determines that the MTS cannot deliver a message to one or more of its immediate recipients, or cannot deliver a report to the originator of its subject message or probe.

A.70 Non-registered Access

In the context of Message Handling Services, access to the service through publicly available telecommunications means by users who have neither been explicitly registered by the service provider, nor been allocated an OR-address.

A.71 Numeric OR-Address

In the context of message handling, an OR-address that numerically identifies a user relative to the ADMD through which the user is accessed. It identifies an ADMD, and a user relative to that ADMD. It is Identifying a user of Message Handling Services by means of a numeric keypad.

A.72 Numeric User Identifier

Standard attribute of an OR-address as a unique sequence of numeric information for identifying a user.

A.73 OR-Address

In the context of message handling, an attribute list that distinguishes one user or DL from another and identifies the user's point of access to MHS or the distribution list's expansion point.

A.74 OR-Name

In the context of message handling, an information object by means of which a user can be designated as the originator, or a user or distribution list designated as a potential recipient of a message or probe. An OR-name distinguishes one user or distribution list from another and can also identify its point of access to MHS.

A.75 Optional User Facilities

In the context of message handling services, the elements of service which are selectable by the user either on a contractual basis (agreed period of time) or on a per-message basis.

NOTE 1 – Optional user facilities are classified as either essential or additional.

NOTE 2 – Essential optional user facilities are to be made available to all message handling users.

NOTE 3 – Additional optional user facilities can be made available for national and international use on the basis of bilateral agreement between the service providers.

A.76 Organization Name

Standard attribute of an OR-address as a unique designation of an organization for the purpose of sending and receiving of messages.

A.77 Organizational Unit Name

Standard attribute of an OR-address as a unique designation of an organizational unit of an organization for the purpose of sending and receiving of messages.

A.78 Originator

In the context of message handling, the user (but not distribution list) that is the ultimate source of a message or probe.

A.79 Personal Name

In the context of message handling, a standard attribute of an OR-address form that identifies a person relative to the entity denoted by another attribute (e.g. an organization name).

NOTE – Components are for example:

- Surname;
- Given name;
- Initials;
- Generation qualifier.

A.80 Physical Delivery (PD)

The delivery of a message in physical form, such as a letter, through a physical delivery system.

A.81 Physical Delivery Access Unit (PDAU)

An Access Unit that subjects messages (but neither probes nor reports) to physical rendition.

A.82 Physical Delivery Address Components

In a postal address they contain the information necessary for the local physical delivery within the physical delivery area of the physical delivery office, i.e. a street address, a P.O. Box address, a poste restante address or a unique name alternatively.

NOTE – The information is generally restricted to one line with up to 30 printable graphic characters. Additional information may be supplied by using the attribute type "extension of physical delivery address component".

A.83 Physical Delivery Country Name

In the context of physical delivery, a unique description of the country of the final destination.

A.84 Physical Delivery Domain

The domain of responsibility of an organization providing a Physical Delivery System and optionally an MTA/PDAU.

A.85 Physical Delivery Office Address Components

In a postal address they contain the information to specify the office which is responsible for the local physical delivery.

NOTE – The information is generally restricted to one line with up to 30 printable graphic characters. In some countries, the postal code will follow the physical delivery office address components in a separate line (possibly together with the country name).

A.86 Physical Delivery Office Name

Standard attribute of a postal OR-address, in the context of physical delivery, specifying the name of the city, village, etc. where the physical delivery office is situated, or where the physical delivery is effected.

A.87 Physical Delivery Office Number

Standard attribute and in a postal OR-address a means to distinguish between more than one physical delivery office within a city, etc.

A.88 Physical Delivery Organization Name

A free form name of the addressed entity in the postal address, taking into account the specified limitations in length.

A.89 Physical Delivery Personal Name

In a postal address, a free form name of the addressed individual containing the family name and optionally the given name(s), the initial(s), title(s) and generation qualifier, taking into account the specified limitations in length.

A.90 Physical Delivery Service

Service provided by a Physical Delivery System.

A.91 Physical Delivery Service Name

Standard attribute of a postal OR-address in the form of the name of the service in the country electronically receiving the message on behalf of the Physical Delivery Service.

A.92 Physical Delivery System (PDS)

A system that performs physical delivery. One important kind of Physical Delivery System is the postal system.

A.93 Physical Message

A physical object comprising a relaying envelope and its content, e.g. a letter.

A.94 Physical Rendition

The transformation of an MHS message to a physical message, e.g. by printing the message on paper and enclosing it in a paper envelope.

A.95 Postal Code

Standard attribute of a postal OR-address to specify the geographical area, and in the context of MHS, used for routing of messages.

A.96 Postal OR-Address

In the context of message handling, an OR-address that identifies a user by means of its postal address. It identifies the physical delivery system through which the user is to be accessed and gives the user's postal address.

A.97 Postal OR-Address Components

They contain in a postal address information to describe the sender or addressee by means of his name (personal name, organization name).

NOTE – In a postal address, the information is generally restricted to one line of 30 printable characters. Additional information may be supplied by using the attribute type "extension of postal OR-address components".

A.98 Post Office Box Address (P.O. Box Address)

A standard attribute in a postal address indicating that physical delivery through a P.O. Box is requested. It carries the P.O. Box number for distribution to the P.O. Box.

A.99 Poste Restante Address

A standard attribute in a postal address indicating that physical delivery at the counter is requested. It may also carry a code.

A.100 Potential Recipient

In the context of message handling, any user or distribution list to which a message or probe is conveyed during the course of transmittal. Equivalently, a preferred member, alternate member, or substitute recipient.

A.101 Private Domain Name

In the context of message handling, a standard attribute of an OR-address form that identifies a PRMD relative to the ADMD denoted by an administration domain name.

A.102 Private Management Domain (PRMD)

A management domain that comprises messaging systems managed by a private organization. While there is no restriction on a PRMD offering public messaging services, the PRMD has not accepted the Administration responsibilities in order to ensure its customers can communicate with any other MD attached to the global messaging backbone.

A.103 Probe

In the context of message handling, an instance of a secondary class of information objects conveyed by means of message transfer that describes a class of messages and that is used to determine the deliverability of such messages.

A.104 Public Message Handling Service

Message Handling Service offered by an Administration.

A.105 Public Services

In the context of telecommunication, the services offered by Administrations.

A.106 Receipt

In the context of message handling, a transmittal step in which either a UA conveys a message or report to its direct user, or the communication system that serves an indirect user conveys such an information object to that user.

A.107 Recipient

See Actual Recipient.

A.108 Recursion

In the context of message handling, the situation that a message gets back to the same distribution list of origin and potentially circulates infinitely.

A.109 Redirection

In the context of message handling, a transmittal event in which an MTA replaces a user among a message's immediate recipients with a user preselected for that message.

A.110 Registered Access

In the context of Message Handling Services, access to the service performed by subscribers who have been registered by the service provider to use the service, and been allocated an OR-address.

A.111 Report

In the context of message handling, an instance of a secondary class of information object conveyed by means of message transfer. It is generated by the MTS, it reports the outcome or progress of a message's or probe's transmittal to one or more potential recipients.

A.112 Retrieval

In the context of message handling, a transmittal step in which a user's message store conveys a message or report to the user's UA. The user is an actual recipient of the message or the originator of the subject message or probe.

A.113 Security Capabilities

In the context of message handling, the mechanisms that protect against various security threats.

A.114 Specialized Access

In the context of message handling, the involvement of specialized Access Units providing intercommunication between Message Handling Services and other telecommunication services.

A.115 Standard Attribute

An attribute whose type is bound to a certain class of information.

A.116 Street Address

A standard attribute in a postal address giving information for the local distribution and physical delivery, i.e. the street name, the street identifier (like street, place, avenue) and the house number.

A.117 Subject

In the context of message handling, the information, part of the header, that summarizes the content of the message as the originator has specified it.

A.118 Subject Message

The message that is the subject of a report.

A.119 Subject Probe

The probe that is the subject of a report.

A.120 Submission

Direct submission or indirect submission.

A.121 Substitute Recipient

In the context of message handling, the user or distribution list to which a preferred, alternate, or member (but not another substitute) recipient had elected to redirect messages (but not probes).

A.122 Terminal Identifier

Standard attribute in an OR-address providing information for identifying a terminal amongst others.

NOTE – An example is the telex answerback.

A.123 Terminal OR-Address

In the context of message handling, an OR-address that identifies a user by means of the network address of his terminal and that can identify the ADMD through which that terminal is accessed. The terminals identified can belong to different networks.

A.124 Terminal Type

Standard attribute of an OR-address that indicates the type of a terminal.

NOTE – Examples: telex, G3 facsimile, G4 facsimile, IA5, videotex terminal.

A.125 Transfer

In the context of message handling, a transmittal step in which one MTA conveys a message, probe, or report to another.

A.126 Transfer System

A messaging system that contains one MTA; optionally one or more Access Units, and neither a UA nor a message store.

A.127 Transmittal

The conveyance or attempted conveyance of a message from its originator to its potential recipients, or of a probe from its originator to MTAs able to affirm any described message's deliverability to its potential recipients. It also encompasses the conveyance or attempted conveyance, to the originator of the message or probe, of any reports it provokes. It is a sequence of transmittal steps and events.

A.128 Unformatted Postal OR-Address

OR-address based on an unformatted postal address.

A.129 Unique Postal Name

In a postal address, a standard attribute describing the point of physical delivery by means of a unique name, e.g. that of a building.

A.130 User

In the context of message handling, a functional object (e.g. a person), a component of the Message Handling Environment, that engages in (rather than provides) message handling and that is a potential source or destination for the information objects an MHS conveys.

A.131 User Agent (UA)

In the context of message handling, the functional object, a component of MHS, by means of which a single direct user engages in message handling.

A.132 Voice Body Part

A body part sent or forwarded from an originator to a recipient which conveys voice encoded data and related information. The related information consists of parameters which are used to assist in the processing of the voice data. These parameters include information detailing the duration of the voice data, the voice encoding algorithm used to encode the voice data, and supplementary information.

Annex B
(informative)

Definitions Of Elements Of Service

NOTE – The abbreviations used in the title line have the following meanings:

MT	Message Transfer
IPM	Interpersonal Messaging
PD	Physical Delivery
MS	Message Store
MS-94	1994 enhanced Message Store
PR	Per Recipient (available on a per-recipient basis)

B.1 Access Management MT

This element of service enables a UA and an MTA to establish access to one another and to manage information associated with access establishment.

The element of service permits the UA and MTA to identify and validate the identity of the other. It provides a capability for the UA to specify its OR-address and to maintain access security. When access security is achieved through passwords, these passwords can be periodically updated.

NOTE – A more secure form of access management is provided by the element of service Secure Access Management.

B.2 Additional Physical Rendition PD PR

This element of service allows an originating user to request the PDAU to provide the additional rendition facilities (e.g. kind of paper, coloured printing, etc.). Bilateral agreement is required to use this element of service.

B.3 Alternate Recipient Allowed MT

This element of service enables an originating UA to specify that the message being submitted can be delivered to an alternate recipient as described below.

A destination MD will interpret all of the user attributes in order to select a recipient UA. Three cases can be distinguished:

1) All the attributes match precisely those of a subscriber UA. Delivery is attempted to that UA.
2) Either insufficient attributes are supplied or those supplied match those of more than one subscriber UA. The message cannot be delivered.
3) At least the minimum set of attributes required by the destination MD is supplied. Nevertheless, taking all of the other attributes into account, the attributes match those of no UA.

In case 3, an MD that supports the Alternate Recipient Assignment Element of Service can deliver the message to a UA that has been assigned to receive such messages. This UA will be notified of the OR-address of the intended recipient as specified by the originator. Delivery to this UA will be reported in a delivery notification, if requested by the originator.

B.4 Alternate Recipient Assignment MT

This element of service enables a UA to be given the capability to have certain messages delivered to it for which there is not an exact match between the recipient attributes specified and the name of the user. Such a UA is specified in terms of one or more attributes for which an exact match is required, and one or more attributes for which any value is acceptable. For example, an organization can establish a UA to receive all messages for which country name, Administration Management Domain name and organization name (for example, company name) are an exact match, but the personal name of the recipient does not correspond to an individual known by an MHS in that organization. This permits the organization to manually handle the messages to these individuals.

In order for a message to be reassigned to an alternate recipient, the originator must have requested the Alternate Recipient Allowed Element of Service.

B.5 Authorization Time Indication IPM

This element of service enables the originator to indicate to the recipient UA the date and time at which a message was formally authorized. Depending upon local requirements, this date and time stamp may vary from the date and time when the message was submitted to the MTS. This element of service may be used to augment the Authorizing Users Indication Element of service (see B.6) to provide supplementary information about the authorizing event.

B.6 Authorizing Users Indication IPM

This element of service allows the originator to indicate to the recipient the names of the one or more persons who authorized the sending of the message. For example, an individual can authorize a particular action which is subsequently communicated to those concerned by another person such as a secretary. The former person is said to authorize its sending while the latter person is the one who sent the message (originator). This does not imply signature-level authorization.

B.7 Auto-acknowledgement of IP-Messages IPM MS-94

This element of service enables an MS-user to instruct the MS to generate a receipt notification automatically for each IP-message containing a receipt notification request which is delivered to the MS. The receipt notification is sent when the complete IP-message has been retrieved by the user or when the user indicates to the MS that he regards the message as having been retrieved.

B.8 Auto-action Log MS-94

This element of service enables an MS-user to access a log that records details of selected auto-action executions performed by the MS. The MS-user is able to retrieve information from the Auto-action Log by means of the Stored Message Listing and Stored Message Fetching Elements of Service. The ability to delete Auto-action Log entries is subject to subscription. This log of information is available if, and only if, this element of service is subscribed to by the user of the MS. Support for an element of service which comprises an auto-action does not require support for the Auto-action Log Element of Service. For each type of auto-action that may generate log entries, it is a subscription option whether all auto-action executions are logged, or only those executions that result in an error, or no executions are logged for that auto-action.

B.9 Auto-advise IPM MS

This element of service enables an MS-user to instruct the MS to generate advice notifications automatically when selected IP-messages are delivered. The notification may inform the originator of the delivered IP-message that the MS-user is absent and, for the present, unable to take receipt of messages, or may intimate a change of address. The notification is generated only if so requested by the IP-message's originator.

B.10 Auto-assignment of Annotations MS-94

This element of service enables an MS-user to instruct the MS to attach annotations to a selected message automatically, when the message is stored in the MS and satisfies specified criteria. The MS-user may specify, through registration, several sets of selection criteria each of which may indicate the attachment of a different value of annotation. Subscription to this element of service requires subscription to the Stored Message Annotation Element of Service.

B.11 Auto-assignment of Group Names MS-94

This element of service enables an MS-user to instruct the MS to assign group names to a selected message automatically, when the message is stored in the MS and satisfies specified criteria. The MS-user may specify, through registration, several sets of selection criteria, each of which may indicate the assignment of a different group name. The MS will verify that only registered group names are assigned to messages. Subscription to this element of service requires subscription to the Stored Message Grouping Element of Service.

B.12 Auto-assignment of Storage Period MS-94

This element of service enables an MS-user to instruct the MS to assign a storage period to a selected message automatically, when the message is stored in the MS and satisfies specified criteria. The MS-user may specify, through registration, several sets of selection criteria each of which may indicate the attachment of a different value of storage period. Subscription to this element of service requires subscription to the Storage Period Assignment Element of Service.

B.13 Auto-correlation of IP-Messages IPM MS-94

This element of service enables an MS-user to retrieve information, automatically generated by the MS, concerning the correlation between various related IP-messages. The following types of messages may be correlated:

1) IP-messages received in reply to, or sent in reply to an IP-message;
2) the IP-messages which forwarded (or auto-forwarded) one or more messages;
3) the received or submitted IP-messages that obsolete an IP-message;
4) the received or submitted IP-messages that indicate that they are related to an IP-message.

Besides identifying each IP-message related to a given message in the ways indicated, the MS provides a summary of all such responding IP-messages.

B.14 Auto-correlation of IP-notifications IPM MS-94

This element of service enables an MS-user to retrieve information, automatically generated by the MS, concerning the IP-notifications that have been received in response to a previously submitted IP-message. Information may also be retrieved concerning IP-notifications sent by the MS-user or the MS in response to delivered IP-messages. The MS identifies each IP-notification related to a given submitted or delivered message, and for submitted messages it also provides a summary of received IP-notifications. This enables the MS-user to access this information directly rather than perform an exhaustive search of all entries that could hold the information. This element of service is effective only if the submitted or delivered message that an IP-notification refers to is stored in the MS, or is recorded in the Submission Log or Delivery Log. Provision for the storage of submitted messages, and maintenance of the Submission Log and the Delivery Log are supported by separate elements of service.

B.15 Auto-correlation of Reports MS-94

This element of service enables an MS-user to retrieve information, automatically generated by the MS, concerning the delivery and non-delivery reports that have been received in response to a previously submitted message. Successful cancellations of deferred delivery for submitted messages are also recorded. In addition to identifying each report related to a given submitted message, the MS provides a summary of these reports. This enables the MS-user to access this information directly rather than perform an exhaustive search of all entries that could hold the information. This element of service requires that at least one of the Submission Log or Storage on Submission Elements of Service has also been subscribed to.

B.16 Auto-deletion After Storage Period MS-94

This element of service enables an MS-user to instruct the MS to delete automatically any stored message whose storage period has elapsed. This registration remains in force until disabled by a subsequent registration. Messages that have not been listed or processed are not subject to auto-deletion. Equally, entries of the Submission Log, Delivery Log, and Auto-action log are not subject to auto-deletion. Other content-specific message handling Specifications may lay down additional rules for the performance of this element of service. Subscription to this element of service requires subscription to the Storage Period Assignment Element of Service.

B.17 Auto-discarding of IP-Messages IPM MS-94

This element of service enables an MS-user to instruct the MS to discard stored IP-messages automatically, if they satisfy criteria registered by the MS-user. An IP-message becomes a candidate for auto-discarding if a subsequently delivered IP-message renders it obsolete, or if it contains an Expiry Time that has been reached. The MS-user may control whether auto-discarding occurs for such IP-messages by specifying additional conditions which the IP-message must satisfy, e.g. that the message has been fetched by the MS-user, or that the obsoleting IP-message has the same originator as the obsoleted IP-message. Where the message has not been fetched by the MS-user before being auto-discarded, a non-receipt notification is generated if requested in the discarded IP-message.

B.18 Auto-forwarded Indication IPM

This element of service allows a recipient to determine that a body of an incoming IP-message contains an IP-message that has been auto-forwarded. Thus the recipient can distinguish from that where an incoming IP-message contains a forwarded message (as described in B.51) in the body. As with a forwarded IP-message, an auto-forwarded IP-message can be accompanied by information (for example, time stamps, indication of conversion) associated with its original delivery.

NOTE – The indication that auto-forwarding of an IP-message has occurred enables a recipient IPM UA, should it so choose, to prevent further auto-forwarding and thus the possibility of loops. In addition, a recipient IPM UA can choose whether or not to auto-forward based on other criteria (for example, sensitivity classification).

When an IPM UA auto-forwards an IP-message, it designates it as auto-forwarded. If receipt/non-receipt notification has been requested for the IP-message being auto-forwarded, the IPM UA generates a non-receipt notification informing the originator of the auto-forwarding of the IP-message. The notification optionally includes a comment supplied by the originally intended recipient. No further notification applying to the auto-forwarded IP-message is generated by any IPM UA.

B.19 Auto-forwarding of IP-Messages IPM MS

This element of service enables an MS-user to instruct the MS to auto-forward selected IP-messages that are delivered to it. The MS-user may specify through registration several sets of criteria chosen from the attributes available in the MS, and IP-messages meeting each set of criteria will be auto-forwarded to one or more users or DLs. If requested by the message originator, a non-receipt notification is generated indicating that the IP-message was auto-forwarded even if the

MS retains a copy of the forwarded message, unless the copy is retained as a new message. For each set of selection criteria, a body part may be specified, to be included as a "cover note" with each auto-forwarded IP-message.

NOTE – In versions of F.400/X.400 and ISO/IEC 10021-1 published prior to 1994, this element of service was named Stored Message Auto-forward, and classified as a general MS optional user facility; it has since been classified as IPM-specific.

B.20 Auto-submitted Indication IPM

This element of service allows the originator, or enables the UA or MS, to indicate to the recipient whether the message was or was not submitted automatically by a machine without either the direct or indirect control by a human of the submission, and to determine the nature of the submission, thus:

— not auto-submitted;

— auto-generated;

— auto-replied.

The absence of this indication yields no information as to whether the message submission involved human control or not.

B.21 Basic Physical Rendition PD PR

This element of service enables the PDAU to provide the basic rendition facilities for converting the MHS message into a physical message. This is the default action to be taken by the PDAU.

B.22 Blind Copy Recipient Indication IPM PR

This element of service allows the originator to provide the OR-name of one or more additional users, or DLs, who are intended recipients of the IP-message being sent. These names are not disclosed to either the primary or copy recipients. Whether or not these additional recipients are disclosed to one another is a local matter.

B.23 Body Part Authentication and Integrity IPM

This element of service allows the originator of the message to provide the recipient with the means by which the recipient can verify that particular body parts of the message have not been modified and that their origin can be authenticated (i.e. a signature).

B.24 Body Part Encryption IPM

This element of service allows the originator to indicate to the recipient that a particular body part of the IP-message being sent has been encrypted. Encryption can be used to prevent unauthorized inspection or modification of the body part. This element of service can be used by the recipient to determine that some body part(s) of the IP-message must be decrypted. The encrypted body part may retain the body part type information, or may be sent in a messaging-system independent format in which there is no information about the type of the information which has been encrypted.

B.25 Circulation List Recipients Indication IPM

This element of service enables the originator to indicate to the recipient a list of recipients to whom it is requested that the IP-message be distributed serially. The circulation list includes an indication of whether each recipient has already received the IP-message. In this context, recipients that have received the message are said to be "checked" in the circulation list. The circulation list should be updated by the recipient and included in an IP-message sent to the next recipient that has not been checked.

B.26 Content Confidentiality MT

This element of service allows the originator of a message to protect the content of the message from disclosure to recipients other than the intended recipient(s). Content Confidentiality is on a per-message basis, and can use either an asymmetric or a symmetric encryption technique.

B.27 Content Integrity MT PR

This element of service allows the originator of the message to provide to the recipient of the message a means by which the recipient can verify that the content of the message has not been modified. Content Integrity is on a per-recipient basis, and can use either an asymmetric or a symmetric encryption technique.

B.28 Content Type Indication MT

This element of service enables an originating UA to indicate the content type for each submitted message. A recipient UA can have one or more content types delivered to it. An example of a content type is the contents generated by the IPM class of co-operating UAs.

B.29 Conversion Prohibition MT

This element of service enables an originating UA to instruct the MTS that implicit encoded information type conversion(s) shall not be performed for a particular submitted message.

B.30 Conversion Prohibition in Case of Loss of Information MT

This element of service enables an originating UA to instruct the MTS that encoded information type conversion(s) shall not be performed for a particular submitted message if such conversion(s) would result in loss of information. Loss of information is discussed in detail in Recommendation X.408.

Should this and the Conversion Prohibition Element of Service both be selected, the latter shall take precedence.

NOTE – This element of service will not protect against possible loss of information in certain cases where the recipient is using an I/O device whose capabilities are unknown to the MTA.

B.31 Converted Indication MT PR

This element of service enables the MTS to indicate to a recipient UA that the MTS performed encoded information type conversion on a delivered message. The recipient UA is informed of the resulting types.

B.32 Counter Collection PD PR

This element of service allows an originating user to instruct the PDS to keep the physical message ready for counter collection at the post office specified by the originator, or at the post office which offers counter collection service closest to the given recipient's address.

B.33 Counter Collection with Advice PD PR

This element of service allows an originating user to instruct the PDS to keep the physical message ready for counter collection at the post office specified by the originator, or at the post office which offers counter collection service closest to the given recipient's address, and to inform the recipient via telephone, or telex, using the number provided by the originator.

B.34 Cover Page Suppression MT PR

This element of service allows the originator to indicate to an Access Unit that a cover page should not be added to the message when it is rendered into physical form. This element of service is particularly intended for facsimile access units, but may also be applied to any other kind of access unit where the basic rendition calls for the AU to generate a cover page.

B.35 Cross-referencing Indication IPM

This element of service allows the originator to associate with the IP-message being sent, the globally unique identifiers of one or more other IP-messages. This enables the recipient's IPM UA, for example, to retrieve from storage a copy of the referenced IP-messages.

B.36 Deferred Delivery MT

This element of service enables an originating UA to instruct the MTS that a message being submitted shall be delivered no sooner than a specified date and time. Delivery will take place as close to the date and time specified as possible, but not before. The date and time specified for deferred delivery is subject to a limit which is defined by the originator's management domain.

B.37 Deferred Delivery Cancellation MT

This element of service enables an originating UA to instruct the MTS to cancel a previously submitted deferred delivery message. The cancellation attempt may or may not always succeed. Possible reasons for failure are: deferred delivery time has passed, or the message has already been forwarded within the MTS.

B.38 Delivery Log MS-94

This element of service enables an MS-user to access a log that records details of the messages and reports delivered to the MS; these records persist even after the messages and reports have been deleted. A Delivery Log entry contains a subset of the information that may be stored for a delivered message. The quantity of information stored in the Delivery Log for each message is specified at subscription time. The MS-user is able to determine whether the delivered message corresponding to a Delivery Log entry has been deleted. The MS-user is able to retrieve information from the Delivery Log by means of the Stored Message Listing, Stored Message Fetching and Stored Message Summary Elements of Service. The ability to delete Delivery Log entries is subject to subscription, and may be restricted to messages meeting certain criteria, e.g. messages stored longer than an agreed period of time.

B.39 Delivery Notification MT PR

This element of service enables an originating UA to request that the originating UA be explicitly notified when a submitted message has been successfully delivered to a recipient UA, or, in the case of access units, may indicate that the message has been successfully received by the destination terminal. The notification is related to the submitted message by means of the message identifier and includes the date and time of delivery. In the case of a multi-destination message, the originating UA can request this element of service on a per-recipient basis.

When a message is delivered after distribution list expansion, then, depending on the policy of the distribution list, the notification can be sent to either the list owner, the message originator, or both.

Delivery notification carries no implication that any UA or user action, such as examination of the message's content, has taken place.

B.40 Delivery Time Stamp Indication MT PR

This element of service enables the MTS to indicate to a recipient UA the date and time at which the MTS delivered a message. In the case of physical delivery, this element of service indicates the date and time at which the PDAU has taken responsibility for printing and further delivery of the physical message.

B.41 Delivery via Bureaufax Service PD PR

This element of service allows an originating user to instruct the PDAU and associated PDS to use the Bureaufax Service for transport and delivery.

B.42 Designation of Recipient by Directory Name MT PR

This element of service enables an originating UA to use a directory name in place of an individual recipient's OR-address.

B.43 Disclosure of Other Recipients MT

This element of service enables the originating UA to instruct the MTS when submitting a multi-recipient message, to disclose the OR-names of all other recipients to each recipient UA, upon delivery of the message. The OR-names disclosed are as supplied by the originating UA. If distribution list expansion has been performed, then only the originator specified DL name will be disclosed, and not the names of its members.

B.44 Distribution Codes Indication IPM

This element of service enables the originator to provide the recipient with information to support its distribution of the IP-message either within the MHS (e.g. auto-forwarding) or external to the MHS (e.g. hard copy distribution). A specific definition of distribution code semantics should be mutually supported by the originator and recipients. Note that this element of service may provide information to auto-actions such as auto-forward and auto-alert.

B.45 DL-exempted Recipients MT

This element of service enables the originator to specify the OR-names of recipients that are requested to be excluded from the set of intended recipients generated as a result of DL expansion. Exclusion is performed at the point of DL expansion. The names of exempted list members are also provided to the remaining recipients. This service does not guarantee that the exempted recipients will not receive the message as the result of other services (e.g. forwarding, redirection).

B.46 DL-expansion History Indication MT

This element of service provides to a recipient, at delivery, information about the distribution list(s) through which the message has arrived. It is a local matter as to how much of this information is presented to the recipient.

B.47 DL-expansion Prohibited MT

This element of service allows an originating user to specify that if any of the recipients can directly or via reassignment refer to a distribution list, then no expansion shall occur. Instead, a Non-delivery Notification will be returned to the originating UA, unless Prevention of Non-delivery Notification has been requested.

B.48 EMS (Express Mail Service) PD PR

This element of service allows an originating user to instruct the PDS to transport and deliver the physical message produced from the MHS message through accelerated letter circulation and delivery service (such as EMS or the equivalent domestic service) in the destination country.

B.49 Expiry Date Indication IPM

This element of service allows the originator to indicate to the recipient the date and time after which he considers the IP-message to be invalid. The intent of this element of service is to state the originator's assessment of the current applicability of an IP-message. The particular action on behalf of a recipient by his IPM UA, or by the recipient himself, is unspecified. Possible actions might be to file or delete the IP-message after the expiry date has passed.

B.50 Explicit Conversion MT PR

This element of service enables an originating UA to request the MTS to perform a specified conversion, such as required when interworking between different Telematic Services. When a message is delivered after conversion has been performed, the recipient UA is informed of the original encoded information types as well as the current encoded information types in the message.

NOTE 1 – This element of service is intended to support interworking with telematic terminals/services.

NOTE 2 – When DL names are used in conjunction with this element of service, conversion will apply to all members of the DL.

B.51 Forwarded IP-message Indication IPM

This element of service allows a forwarded IP-message, or a forwarded IP-message plus its "delivery information" to be sent as the body (or as one of the body parts) of an IP-message. An indication that the body part is forwarded is conveyed along with the body part. In a multi-part body, forwarded body parts can be included along with body parts of other types. "Delivery information" is information which is conveyed from the MTS when an IP-message is delivered (for example, time stamps and indication of conversion). However, inclusion of this delivery information along with a forwarded IP-message in no way guarantees that this delivery information is validated by the MTS.

The Receipt Notification Request Indication and the Non-receipt Notification Request Elements of Service are not affected by the forwarding of an IP-message.

B.52 Grade of Delivery Selection MT

This element of service enables an originating UA to request that transfer through the MTS be urgent or non-urgent, rather than normal. The time periods defined for non-urgent and urgent transfer are longer and shorter, respectively, than that defined for normal transfer. This indication is also sent to the recipient with the message.

B.53 Hold for Delivery MT

This element of service enables a recipient UA to request that the MTS hold its messages and returning notifications for delivery until a later time. The UA can indicate to the MTS when it is unavailable to take delivery of messages and notifications, and also, when it is again ready to accept delivery of messages and notifications from the MTS. The MTS can indicate to the UA that messages are waiting due to the criteria the UA established for holding messages. Responsibility for the management of this element of service lies with the recipient MTA.

Criteria for requesting a message to be held for delivery are: encoded information type, content type, maximum content length and priority. The message will be held until the maximum delivery time for that message expires, unless the recipient releases the hold prior to its expiry.

NOTE – The Hold for Delivery Element of Service is distinct from the message store facility. The Hold for Delivery Element of Service provides temporary storage to facilitate delivery and only after a message has been transferred to the recipient's UA is delivery notification returned. The message store facility augments the storage of a UA and can be used to store messages for an extended period of time. Unlike the Hold for Delivery Element of Service, delivery notifications are returned as soon as the message is placed in (that is, delivered to) the message store.

B.54 Implicit Conversion **MT**

This element of service enables a recipient UA to have the MTS perform for a period of time any necessary conversion on messages prior to delivery. Neither the originating nor recipient UA explicitly requests this element of service on a per-message basis. If the encoded information type capabilities of the recipient UA are such that more than one type of conversion can be performed, the most appropriate conversion is performed. When a message is delivered after conversion has been performed, the recipient UA is informed of the original encoded information types as well as the current encoded information types in the message.

B.55 Importance Indication **IPM**

This element of service allows the originator to indicate to the recipients his assessment of the importance of the IP-message being sent. Three levels of importance are defined: *low*, *normal* and *high*.

This element of service is not related to the Grade of Delivery Selection Element of Service provided by the MTS. The particular action taken by the recipient or his IPM UA based on the importance categorization is unspecified. It is the intent to allow the recipient IPM UA, for example, to present IP-messages in order of their importance or to alert the recipient of the arrival of IP-messages of high importance.

B.56 Incomplete Copy Indication **IPM**

This element of service allows an originator to indicate that this IP-message is an incomplete copy of an IP-message with the same IP-message identification in that one or more body parts, and/or heading fields of the original IP-message are absent.

B.57 Information Category Indication **IPM**

This element of service enables the originator to indicate to the recipient the character of the information contained in the IP-message. The service can provide a registered identifier for each particular category, or free form information describing the nature of the communication. The recipients may use the information provided by this service to affect the presentation of messages to the recipient, or to affect any other local processing functions. A specific definition of information category values and semantics should be mutually supported by the originator and the recipient. Examples of information categories include: *draft message*, *press release*, *contractual commitment*, *policy statement*.

B.58 IP-message Action Status **IPM MS-94**

This element of service enables an MS-user to determine whether a reply or a receipt notification has been requested of the user in an IP-message which the user has received. It allows the user to record in the MS (and subsequently retrieve the information) that the reply (or IP-notification) has been sent. In addition, the user may set a reminder that a reply is intended even if no reply was explicitly requested.

B.59 IP-message Identification **IPM**

This element of service enables co-operating IPM UAs to convey a globally unique identifier for each IP-message sent or received. The IP-message identifier is composed of an OR-name of the originator and an identifier that is unique with respect to that name. IPM UAs and users use this identifier to refer to a previously sent or received IP-message (for example, in receipt notifications).

B.60 IP-message Security Labelling IPM

This element of service augments the Message Security Labelling service (see B.67) by allowing the originator of an IP-message to convey to all recipients an indication of the security classification of the IP-message content, or optionally, of the component heading and body parts of an IP-message. This service enables the implementation of security policies in which the security labels associated with local objects (e.g. files) derived from component parts of the IP-message may be assigned values provided by the originating IPM user. The integrity of the IP-message Security Labelling may be provided by the Content Integrity or Body Part Authentication and Integrity security service, and confidentiality of the IP-message Security Labelling may be provided by the Content Confidentiality security service. Authentication of the originator of the IP-message Security Labelling may be provided by the Message Origin Authentication service or the Body Part Authentication and Integrity service.

NOTE 1 – Unless both end systems have mutual trust in each end system's ability to process and separate information based on security labels, this label should not be used to implement mandatory access control.

NOTE 2 – The meaning of the term "security classification" in this context is relative to the specific security policy in force.

B.61 Language Indication IPM

This element of service enables an originating UA to indicate the language type(s) of a submitted IP-message.

B.62 Latest Delivery Designation MT

This element of service enables an originating UA to specify the latest time by which the message is to be delivered. If the MTS cannot deliver by the time specified, the message is not delivered and is cancelled. On multi-recipient messages, the latest delivery time can expire prior to delivery to all recipients, but this will not negate any deliveries which have already occurred.

B.63 Manual Handling Instructions Indication IPM

This element of service enables the originator to indicate to the recipient instructions for manual handling of the IP-message, following its delivery. The service can provide instructions consisting of free form text. Examples of manual handling instructions include special recipient handling requests (e.g. "Please pass to...", "Please DO NOT pass to..."), and instructions on how to process body data.

NOTE – Instructions indicated by this element of service may apply either to the IP-message as a whole or to specific components of the IP-message. Where necessary, the content of the instructions should indicate the scope of the instructions or the part(s) of the IP-message to which the instruction applies.

B.64 Message Flow Confidentiality MT

This element of service allows the originator of the message to protect information which might be derived from observation of the message flow.

NOTE – Only a limited form of this is supported.

B.65 Message Identification MT

This element of service enables the MTS to provide a UA with a unique identifier for each message or probe submitted or delivered by the MTS. UAs and the MTS use this identifier to refer to a previously submitted message in connection with Elements of Service such as Delivery and Non-delivery Notification.

B.66 Message Origin Authentication MT PR

This element of service allows the originator of a message to provide to the recipient(s) of the message, and any MTA through which the message is transferred, a means by which the origin of the message can be authenticated (i.e. a signature). Message Origin Authentication can be provided to the recipient(s) of the message, and any MTA through which the message is transferred, on a per-message basis using an asymmetric encryption technique, or can be provided only to the recipient(s) of the message, on a per-recipient basis using either an asymmetric or a symmetric encryption technique.

B.67 Message Security Labelling MT

This element of service allows the originator of a message (or probe) to associate with the message (and any reports on the message or probe) an indication of the sensitivity of the message (a security label). The message security label may be used by the MTS and the recipient(s) of the message to determine the handling of the message in line with the security policy in force.

B.68 Message Sequence Integrity MT PR

This element of service allows the originator of the message to provide to a recipient of the message a means by which the recipient can verify that the sequence of messages from the originator to the recipient has been preserved (without message loss, re-ordering, or replay). Message Sequence Integrity is on a per-recipient basis, and can use either an asymmetric or a symmetric encryption technique.

B.69 MS Register MS

This element of service enables an MS-user to register various items of information with the MS in order to modify certain aspects of its behaviour, such as:

1) the performance of automatic actions;
2) the default set of information retrieved when using the Stored Message Fetching and Stored Message Listing Elements of Service. One set of information may be registered per UA employed by the user;
3) the credentials used by the Message Store to authenticate the MS-user.

If a user employs more than one UA implementation, then as a subscription option the MS may store a separate set of registration information for each UA. The user may retrieve the registered information from the MS.

NOTE – The capability to store separate sets of registration information and to retrieve registered information was not defined in versions of this part of ISO/IEC 10021 published prior to 1994.

B.70 Multi-destination Delivery MT PR

This element of service enables an originating UA to specify that a message being submitted is to be delivered to more than one recipient UA. Simultaneous delivery to all specified UAs is not implied by this element of service.

B.71 Multi-part Body IPM

This element of service allows an originator to send to a recipient or recipients an IP-message with a body that is partitioned into several parts. The nature and attributes, or type, of each body part are conveyed along with the body part.