5i’

FASCICLE II.6

Recommendations F.400-F.422, F.500

MESSAGE HANDLING AND DIRECTORY SERVICES —

OPERATIONS AND DEFINITION OF SERVICE

MONTAGE PAGE 2 = PAGE BLANCHE

PROTECTION OF THE COMMON NAMES OF

CCITT DEFINED INTERNATIONAL PUBLIC SERVICES

Resolution No. 13 published in Volume I is reproduced below for the convenience of the reader.

Resolution No. 13

PROTECTION OF THE COMMON NAMES OF CCITT DEFINED

INTERNATIONAL PUBLIC SERVICES

(Geneva, 1980)

The CCITT,

considering

(a) that CCITT has defined, *inter alia* , the international public services ‘‘ teletex telefax ´bureaufax ´Service Recommendations;

(b) that those international public services are characterized by complete end-to-end compatibility;

(c) that it is desirable to use on a worldwide basis for those CCITT defined international public services their respective common name, i.e. ‘‘teletex’’, ‘‘telefax’’ or ‘‘bureaufax’’, to qualify any service provided in that respect as complying completely with the CCITT definitions for the respective international public service in order to guarantee end-to-end compatibility;

(d) that it is essential to protect the use of the aforementioned common names;

noting

(a) that within a number of countries, several Recognized Private Operating Agencies (RPOAs) may provide such CCITT defined international public services and may also wish to add further optional user facilities in addition to the respective basic international public service as defined by the CCITT;

(b) that, for the preceding reason, some RPOAs may wish to use service designations, e.g. XXX/teletex, indicating a combination of a basic international public service as defined by the CCITT with additional optional user facilities;

resolves to request Administrations

(1) to ensure that any such international public service offered by an Administration be denominated by its respective common name, i.e. ‘‘teletex’’, ‘‘telefax’’ or ‘‘bureaufax’’ and comply completely with the respective CCITT definitions for such service;

(2) to endeavour to protect the common names of the CCITT defined international public services ‘‘teletex’’, ‘‘telefax’’ and ‘‘bureaufax’’, *inter alia* through the communication of those names to the national, regional and international authorities for the registration and administration of trade marks and service marks in order to ensure that the said names be not made the subject of trade marks or service marks or if claimed in an application for the registration of trade marks or service marks be made the subject of a disclaimer;

(3) to ensure that in the case of a combination of any such CCITT defined international public services together with further optional user facilities in addition to that basic service, the trade mark or the service mark for such a combined service offered by any RPOA be always combined with the respective common name of the basic CCITT defined international public

service, i.e. ‘‘teletex’’, ‘‘telefax’’ or ‘‘bureaufax’’, and that the latter names, in the case of registration of such a trade mark or service mark, be made the subject of a disclaimer;

(4) to inform the Director of the CCITT continuously about the measures taken with regard to resolves (1) to (3) above;

requests the Director of the CCITT

to compile the information received in respect of such measures and to make this information available on request for consultation by Administrations.

BLANC

SECTION 1

MESSAGE HANDLING SERVICES

Recommendation F.400

MESSAGE HANDLING SYSTEM AND SERVICE OVERVIEW

The establishment in various countries of telematic services and computer based store and forward messaging services in association with public networks creates a need to produce standards to facilitate international message exchange between subscribers to such services.

The CCITT,

considering

(a) the need for message handling systems;

(b) the need to transfer and store messages of different types;

(c) that Recommendation X.200 defines the reference model of open systems interconnection for CCITT applications;

(d) that Recommendations X.208, X.217, X.218 and X.219 provide the foundation for CCITT applications;

(e) that the X.500-Series Recommendations define directory systems;

(f) that message handling systems are defined in a series of Recommendations: X.400, X.402, X.403, X.407, X.408, X.411, X.413 and X.419;

(g) that interpersonal message is defined in Recommendation X.420 and T.330;

(h) that several F-Series Recommendations describe public message handling services: F.400, F.401, F.410 and F.420;

(i) that several F-Series Recommendations describe intercommunication between public message handling services and other services: F.421, F.415 and F.422,

unanimously declares

the view that the overall system and service overview of message handling is defined in this Recommen dation.

Recommendation X.400 is identical to F.400.

CONTENTS

PART 1 — INTRODUCTION

0 Introduction

This Recommendation is one of a set of Recommendations for message handling. The entire set provides a comprehensive specification for message handling comprising any number of cooperating 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) cooperate 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. other telematic services, postal services).

This Recommendation specifies the overall system and service description of message handling capabilities.

1 Scope

This Recommendation 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 Recommendations. The layout of Recommendations defining the message handling system and services is shown in Table 1/F.400. The public services built on MHS, as well as access to and from the MHS for public services are defined in the F.400-Series of Recommendations.

The technical aspects of MHS are defined in the X.400-Series of Recommendations. The overall system architecture of MHS is defined in Recommendation X.402.

BLANC

H.T. [T1.400]

TABLE 1/F.400

Structure of MHS Recommendations

{

	Joint MHS CCITT	Joint support ISO	CCITT only CCITT	ISO	System	Service	
MHS:	System and service overview	X.400	10021-1				F.400
MHS:	Overall architecture	X.402	10021-2				
MHS:	Conformance testing					X.403	
MHS:	{						
Abstract service definition conventions							
}	X.407	10021-3					
MHS:	{						
Encoded information type conversion rules							
}					X.408		
MHS:	{						
MTS:							
Abstract service definition and procedures							
}	X.411	10021-4					
MHS:	{						
MS:							
Abstract service definition							
}	X.413	10021-5					
MHS:	Protocol specifications	X.419	10021-6				
MHS:	{						
Interpersonal messaging system							
}	X.420	10021-7					
Telematic access to IPMS					T.330		
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 teletex							
}						F.422	
OSI:	Basic reference model			X.200	7498		
OSI:	{						
Specification of abstract syntax notation one (ASN.1)							
}			X.208	8824			
OSI:	{						
Specification of basic encoding rules for abstract syntax notation one (ASN.1)							
}			X.209	8825			
OSI:	{						
Association control: service definition							
}			X.217	8649			
OSI:	{						
Reliable transfer: model and service definition							
}			X.218	9066-1			
OSI:	{						
Remote operations: model, notation and service definition							
}			X.219	9072-1			
OSI:	{						
Association control: protocol specification							
}			X.227	8650			

OSI: Reliable transfer: protocol specification }	{		X.228	9066-2				
OSI: Remote operations: protocol specification }	{		X.229	9072-2				

Tableau 1/F.400 [T1.400], p. 1

2 References

This Recommendation cites the documents listed below:

Recommendation F.60	Operational provisions for the international telex service
Recommendation F.69	Plan for the telex destination codes
Recommendation F.72	International telex store-and-forward — General principles and operational aspects
Recommendation F.160	General operational provisions for the international public fascimile services
Recommendation F.200	Teletex service
Recommendation F.300	Videotex service
Recommendation F.400	Message handling — System and service overview (see also ISO 10021-1)
Recommendation F.401	Message handling services — Naming and addressing for public message handling services
Recommendation F.410	Message handling services — The public message transfer service
Recommendation F.415	Message handling services — Intercommunication with public physical delivery services
Recommendation F.420	Message handling services — The public interpersonal messaging service
Recommendation F.421	Message handling services — Intercommunication between the IPM service and the telex service
Recommendation F.422	Message handling services — Intercommunication between the IPM service and the teletex service
Recommendation T.61	Character repertoire and coded character sets for the international teletex service
Recommendation T.330	Telematic access to IPMS
Recommendation U.80	International teletex store-and-forward — Access from telex
Recommendation U.204	Interworking between the telex service and the public interpersonal messaging service
Recommendation X.200	Reference model of open systems interconnection for CCITT applications (see also ISO 7498)
Recommendation X.208	Specification of abstract syntax notation one (ASN.1) (see also ISO 8824)
Recommendation X.209	Specification of basic encoding rules for abstract syntax notation one (ASN.1) (see also ISO 8825)
Recommendation X.217	Association control: Service definitions (see also ISO 8649)
Recommendation X.218	Reliable transfer model: Service definition (see also ISO/IEC 9066-1)
Recommendation X.219	Remote operations model: Notation and service definition (see also ISO/IEC 9072-1)
Recommendation X.400	Message handling — System and service overview (see also ISO/IEC 10021-1)
Recommendation X.402	Message handling systems — Overall architecture (see also ISO/IEC 10021-2)
Recommendation X.403	Message handling systems — Conformance testing
Recommendation X.407	Message handling systems — Abstract service definition conventions (see also ISO/IEC 10021-3)
Recommendation X.408	Message handling systems — Encoded information type convention rules
Recommendation X.411	Message handling systems — Message transfer system: Abstract service definition and procedures (see also ISO/IEC 10021-4)

Recommendation X.413	Message handling systems — Message store: Abstract service definition (see also ISO/IEC 10021-5)
Recommendation X.419	Message handling systems — Protocol specifications (see also ISO/IEC 10021-6)
Recommendation X.420	Message handling systems — Interpersonal messaging system (see also ISO/IEC 10021-7)
Recommendation X.500	Directory — Overview (see also ISO/IEC 9594-1)
Recommendation X.501	Directory — Models (see also ISO/IEC 9594-2)
Recommendation X.509	Directory — Authentication (see also ISO/IEC 9594-8)
Recommendation X.511	Directory — Abstract service definition (see also ISO/IEC 9594-3)
Recommendation X.518	Directory — Procedures for distributed operations (see also ISO/IEC 9594-4)
Recommendation X.519	Directory — Protocol specifications (see also ISO/IEC 9594-5)
Recommendation X.520	Directory — Selected attribute types (see also ISO/IEC 9594-6)
Recommendation X.521	Directory — Selected object classes (see also ISO/IEC 9594-7)

3 Definitions

This Recommendation uses the terms listed below, and those defined in Annex A.

Definitions of the elements of service applicable to MHS are contained in Annex B.

3.1 *Open systems interconnection*

This Recommendation uses the following terms defined in Recommendation X.200:

a) Application layer;

b) Application-process;

c) Open systems interconnection;

d) OSI reference model.

3.2 *Directory systems*

This Recommendation uses the following terms defined in Recommendation X.500:

a) directory entry;

b) directory system agent;

c) directory system;

d) directory user agent.

This Recommendation uses the following terms defined in Recommendation X.501:

e) attribute;

f) group;

g) member;

h) 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
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
O/R	Originator/recipient
OSI	Open system 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
TLMA	Telematic agent
TLXAU	Telex access unit
TTX	Teletex
UA	User agent

5 Conventions

In this Recommendation the expression ‘‘Administration’’ is used for shortness to indicate a telecommunication Administration, a recognized private operating agency, and, in the case of intercommunication with public delivery service, a postal Administration.

Note — This Recommendation is identical to Recommendation X.400. Because of the desired alignment with ISO, the conventions of ISO standards have been adopted for the structure of this text. These conventions differ from the CCITT style. The other Recommendations of the F.400-Series are in accordance with CCITT conventions.

BLANC

PART 2 — GENERAL DESCRIPTION OF MHS

6 Purpose

This Recommendation is one of a set of Recommendations and describes the system model and elements of service of the message handling system (MHS) and services. This Recommendation overviews the capabilities of an MHS that are used by Administrations for the provision of public 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) for CCITT applications (Recommendation X.200) 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.

Message handling services provided by Administrations belong to the group of telematic services defined in F-Series Recommendations.

Various other telematic services and telex (Recommendations F.60, F.160, F.200, F.300, etc.), data transmission services (X.1), or physical delivery services (F.415) gain access to, and intercommunicate with, the IPM service or intercommunicate with each other, via access units.

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 Recommendations 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/F.400. 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 shown in Figure 1/F.400. The MS is a functional entity whose primary purpose is to store and permit retrieval of delivered messages. The MS also allows for submission from, and alerting to the UA.

The collection of UAs, MSs, AUs and MTAs is called the message handling system (MHS).

Figure 1/F.400, p. 2

7.2 *Structure of messages*

The basic structure of messages conveyed by the MTS is shown in Figure 2/F.400. 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 delivered to one or more recipient UAs. The MTS neither modifies or examines the content, except for conversion (see § 16).

Figure 2/F.400, p. 3

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 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/F.400 and 4/F.400. The different physical systems can be connected by means of dedicated lines or switched network connections.

Figure 3/F.400, p. 4

Figure 4/F.400, p. 5

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 operated by an Administration or organization constitutes a management domain (MD). An MD managed by an Administration is called an Administration management domain (ADMD). An MD managed by an organization other than an Administration is called a private management domain (PRMD). An MD provides message handling services in accordance with the classification of elements of service as described in § 19. The relationships between management domains is shown in Figure 5/F.400.

Figure 5/F.400, p.

Note 1 — It should be recognized that the provision of support of private messaging systems by CCITT members falls within the framework of national regulations. Thus the possibilities mentioned in this paragraph may or may not be offered by an Administration which provides message handling services. In addition, the UAs depicted in Figure 5/F.400 do not imply that UAs belonging to an MD must be exclusively located in the same country as their MDs.

Note 2 — Direct interactions between PRMDs and internal interactions within an MD are outside the scope of this Recommendation.

Note 3 — An Administration, in the context of CCITT, that manages an ADMD, is understood as being a member of ITU or a recognized private operating agency (RPOA), registered by a country with the ITU.

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 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:

— users to Administration provided UA

— private UA to Administration MTA

— private UA to Administration MS

— private UA to Administration MTA

— user to Administration provided UA.

See also the examples of configurations shown in Figure 3/F.400 and Figure 4/F.400.

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 an PRMD can access one or more ADMDs in a country, following national regulations.

Access can also be provided by Administration provided AUs described in §§ 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 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 is considered to exist entirely within one country. Within that country, the PRMD can have access to one or more ADMDs as shown in Figure 5/F.400. 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 will not act as a relay between two ADMDs.

In the interaction between a PRMD and an ADMD, the ADMD takes responsibility for the actions of the PRMD which are related to the interaction. In addition to ensuring that the PRMD properly provides the message transfer service, the ADMD is responsible for ensuring that the accounting, logging, quality of service, uniqueness of names, and related operations of the PRMD are correctly performed. 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.

7.4 *Message store*

Because UAs can be implemented on a wide variety of equipment, including personal computers, the MS can complement a UA implemented, for example, on a personal computer by providing a more secure, continuously available storage mechanism to take delivery of messages on the user agent's behalf. The MS retrieval capability provides users who subscribe to an MS with basic message retrieval capabilities potentially applicable to messages of all types. Figure 6/F.400 shows the delivery, and subsequent retrieval of messages that are delivered to an MS, and the indirect submission of messages via the MS.

Figure 6/F.400, p.

One MS acts on behalf of only one user (one O/R address), i.e. it does not provide a common or shared MS capability to several users (see also PRMD3 of Figure 5/F.400).

When subscribing to an MS, all messages destined for the UA are delivered to the MS only. The UA, if on line, can receive alerts when certain messages are delivered to the MS. Messages delivered to an MS are considered delivered from the MTS perspective.

When a UA submits a message through the MS, the MS is in general transparent and submits it to the MTA before confirming the success of the submission to the UA. However, the MS can expand the message if the UA requests the forwarding of messages that exist in the MS.

Users are also provided with the capability to request the MS to forward selected messages automatically upon delivery.

The elements of service describing the features of the MS are defined in Annex B and classified in § 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.

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. In the case of Administration supplied MSs, the subscriber either provides his own UA or makes use of an Administration supplied UA via an I/O device. In either case, 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 cases can exist.

8 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 § 19. Provision of public message transfer service by Administrations is described in Recommendation F.410.

8.1 *Submission and delivery*

The MTS provides the means by which UAs exchange messages. There are two basic interactions between MTAs and UAs and/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 recipient's 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 the 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 not 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 acknowledgement 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 can submit messages through it, and retrieve messages that have been delivered to the MS.

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 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 § 9, is one example of this. Other services can be built on the foundation of the MTS, either with corresponding recommendations or as private applications.

9 IPM service

The interpersonal message 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 § 19. The provision of public interpersonal messaging service by Administrations is described in Recommendation F.420.

9.1 *IPM service functional model*

Figure 7/F.400 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 (TLMA, PTLXAU) allow for teletex and telex

users to intercommunicate with the IPM service. The optional access unit (TLMA) also allows for teletex users to participate in the IPM service (see also § 11). 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 IP 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 release to the basic message structure of MHS is shown in Figure 8/F.400. The IP-message is conveyed with an envelope when being transferred through the MTS.

Figure 9/F.400 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 which can be of a different encoded information type, such as voice, text, facsimile and graphics.

Figure 7/F.400, p. 8

Figure 8/F.400, p. 9

Figure 9/F.400, p. 10

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 (such as reading/not reading the message) recipient action. In certain cases the non-receipt notification is generated automatically by the recipient's UA.

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., hardcopy) 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 for further study. 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 10/F.400 shows the functional model of this interworking. Provision of intercommunication between public message handling services offered by Administrations and PD services is described in Recommendation F.415. The elements of service describing the features of this intercommunication are defined in Annex B/F.400 and classified in § 19.

Figure 10/F.400, p.

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 address form appropriate for this exists and is described in § 12.

10.2 *Organizational configurations*

Possible organizational mappings of the functional model described above are shown in Figure 11/F.400. In each model (A & 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.

11 Specialized access

11.1 *Introduction*

The functional model of MHS (Figure 1/F.400) 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 in 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 PDU described in § 10.

Other forms of access are described below.

Figure 11/F.400, p. 12

11.2 *Teletex access*

11.2.1 *Registered access to the IPM service*

The specialized access unit defined for telematic access — telematic agent (TLMA) caters specially for teletex (TTX) terminals. This TLMA provides for teletex access to the IPM service as shown in Figure 7/F.400. The technical provisions of this access are defined in Recommendation T.330. The TLMA enables users of teletex terminals to participate fully in the IPM service.

11.2.2 *Non-registered (public) access to the IPM service*

The specialized access unit defined for telematic access — telematic agent (TLMA) also provides for public access to the IPM service for TTX users who are not registered users of the IPM service. This is shown in Figure 7/F.400. The technical provisions of this access are defined in Recommendation T.330. The intercommunication between the IPM service and the teletex service is defined in Recommendation F.422.

11.3 *Telex access*

11.3.1 *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.

11.3.2 *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 7/F.400. 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. The intercommunication between the IPM service and the telex service is defined in Recommendation F.421.

Note — Other types of access units are for further study (e.g., facsimile, videotex, etc.).

PART 3 — CAPABILITIES OF MHS

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 O/R names. O/R names are comprised of directory names and/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 O/R address. The structure and components of directory names are described in the X.500-Series of Recommendations.

A user can access a directory system directly to find out the O/R address of a user, or O/R 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 O/R address or addresses automatically as described in § 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 *O/R names*

Every MH user or DL will have one or more O/R name(s). An O/R name comprises a directory name, and O/R address, or both.

Either or both components of an O/R 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 O/R address, which it will then use to route and deliver the message. If a directory name is absent, it will use the O/R address as given. When both are given on submission, MHS will use the O/R address, but will carry the directory name and present both to the recipient. If the O/R address is invalid, it will then attempt to use the directory name as above.

12.4 *O/R addresses*

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

An O/R address is a collection of information called attributes. Recommendation X.402 specifies a set of standard attributes from which O/R addresses can be constructed. Standard attributes mean that their syntax and semantics are defined in Recommendation X.402. 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 O/R addresses are defined, each serving their own purpose. These forms and their purpose are as follows:

— *Mnemonic O/R 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 O/R address:* Provides a means of identifying users with terminals belonging to various networks.

— *Numeric O/R address:* Provides a means of identifying users by means of numeric keypads.

— *Postal O/R address:* Provides a means of identifying originators and recipients of physical messages.

13 MHS use of directory

13.1 *Introduction*

The directory defined by the X.500-Series of Recommendations provides capabilities useful in the use and provision of a variety of telecommunication services. This clause describes how a directory can be used in messages handling. Details can be found in other X.400 Recommendations.

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 O/R 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 O/R 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 O/R 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 O/R address. The UA can then supply both the directory name and the O/R 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 O/R address and add it to the envelope. The originating MTA normally carries out the name to O/R address look up.

A functional model depicting the above is shown in Figure 12/F.400.

Figure 12/F.400, p.

13.3 *Physical configurations*

Some possible physical configurations of the above functional model are shown in Figure 13/F.400. Where a directory user agent (DUA) and directory system agent (DSA) reside in physically separate systems, a standard directory protocol, defined in the X.500-Series of Recommendations, 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/F.400, p.

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 an unambiguous O/R address. This O/R address identifies the expansion point, which is the 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 14/F.400.

— *DL owner:* A user who is responsible for the management of a DL.

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 O/R name, the directory name, the O/R address, or both (see § 12 for details). The originator need not be aware that the O/R 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 to the list of recipients of the message and transmit the message to them.

Figure 14/F.400, p.

14.6 *Nesting*

A member of a DL can be another DL as shown in Figure 14/F.400. In this case the message is forwarded from the expansion point of the parent DL to the expansion point of the member 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 14/F.400) rather than that of the message originator, is compared against the submit permission of the member DL (e.g., DL2 in Figure 14/F.400).

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 or DLs he got 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 got the message, or both, as shown in Figure 15/F.400.

Figure 15/F.400, p.

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.

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 this 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 imposer 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 the 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. Security capabilities to protect MH user-to-MH user communication are for further study.

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 an 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 recipients' UAs.

The scope of the secure messaging elements of service is given in Table 2/F.400. 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 Recommendation describes the use of security services by the UA, and the MTA. How these features are applied to access units is for further study.

15.4 *MHS security capabilities*

The elements of service describing the security features of MHS are defined in Annex B, and classified in § 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.

H.T. [T2.400]

TABLE 2/F.400

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**
The MHS component is a provider of the service.			
The MHS component is a user of the service.			

Table 2/F.400 [T2.400], p.

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 Recommendation X.509. The directory stores certified copies of public keys for MHS 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 Recommendation X.519.

Recommendations for other types of key management schemes, including symmetric encryption, to support the security features are for further study.

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 Recommendation X.411. Conversions and the use of the elements of service relating to conversion are available for EITs not defined in Recommendation X.411, but supported by certain domains, either bilaterally between these domains or within a domain itself.

MHS 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 Recommendation X.408.

Recommendation X.408 deals with conversion for the following: telex, IA5 text, teletex, G3fax, G4 Class1, videotex, voice, and mixed mode.

17 Use of the MHS in provision of public services

The message handling system is used in the provision of public MH services that are offered by Administrations for use by their subscribers. These public MH services are defined in the F.400-Series Recommendations and include:

— the public message transfer service (Rec. F.410);

— the public interpersonal messaging service (Rec. F.420).

In addition complementary public services are offered by Administrations to allow for the intercommunication between CCITT services and the public MH services mentioned above, as follows:

— intercommunication with public physical delivery services (Rec. F.415).

— intercommunication between the IPM service and the telex service (Rec. F.421);

— intercommunication between the IPM service and the teletex service (Rec. F.422);

Recommendation F.401 describes the naming and addressing aspects for public MH services.

BLANC

PART 4 — ELEMENTS OF SERVICE

18 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 Recommendations in the X.400 Series.

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 3/F.400 lists all the elements of service available in MHS, shows what service they are specifically associated with of the presently defined services, MT service, IPM service, and PD service, or whether they are specific to the message store, and gives the corresponding reference number to the definition in Annex B.

BLANC

H.T. [1T3.400]
TABLE 3/F.400
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
Authorizing users indication		X			B.5
Auto-forwarded indication		X			B.6
Basic physical rendition			X		B.7
{ Blind copy recipient indication }		X			B.8
{ Body part encryption indication }		X			B.9
Content confidentiality	X				B.10
Content integrity	X				B.11
Content type indication	X				B.12
Conversion prohibition	X				B.13
{ Conversion prohibition in case of loss information }	X				B.14
Converted indication	X				B.15
Counter collection			X		B.16
{ Counter collection with advice }			X		B.17
{ Cross-referencing indication }		X			B.18
Deferred delivery	X				B.19
{ Deferred delivery cancellation }	X				B.20
Delivery notification	X				B.21
{ Delivery time stamp indication }	X				B.22
{ Delivery via Bureaufax service }			X		B.23
{ Designation of recipient by directory name }	X				B.24
{ Disclosure of other recipients }	X				B.25
{ DL expansion history indication }	X				B.26
DL expansion prohibited	X				B.27
EMS (express mail service)			X		B.28
Expiry date indication		X			B.29
Explicit conversion	X				B.30
{ Fowarded IP-message indication }		X			B.31
Garde of delivery selection	X				B.32
Hold for delivery	X				B.33
Implicit conversion	X				B.34
Importance indication		X			B.35

Incomplete copy indication		X			B.36
IP-message identification		X			B.37
Language indication		X			B.38
Latest delivery designation	X				B.39
Message flow confidentiality	X				B.40
Message identification	X				B.41
Message origin authentication	X				B.42
Message security labelling	X				B.43
Message sequence integrity	X				B.44
Multi-destination delivery	X				B.45
Multi-part body		X			B.46
Non-delivery notification	X				B.47

Tableau 3/F.400 [1T3.400], p. 18

H.T. [2T3.400]

TABLE 3/F.400 *(cont.)*

Elements of service	MT	IPM	PD	MS	Annex B reference
{ Non-receipt notification request indication }		X			B.48
{ Non-repudiation of delivery }	X				B.49
Non-repudiation of origin	X				B.50
{ Non-repudiation of submission }	X				B.51
Obsoleting indication		X			B.52
Ordinary mail			X		B.53
{ Original encoded information types indication }	X				B.54
Originator indication		X			B.55
{ Originator requested alternate recipient }	X				B.56
{ Physical delivery notification by MHS }			X		B.57
{ Physical delivery notification by PDS }			X		B.58
Physical forwarding allowed			X		B.59
Physical fowarding prohibited			X		B.60
{ Prevention of non-delivery notification }	X				B.61
{ Primary and copy recipients indication }		X			B.62
Probe	X				B.63
Probe origin authentication	X				B.64
Proof of delivery	X				B.65
Proof of submission	X				B.66
{ Receipt notification request indication }		X			B.67
{ Redirection disallowed by originator }	X				B.68
{ Redirection of incoming messages }	X				B.69
Registered mail			X		B.70
{ Registered mail to addressee in person }			X		B.71
Reply request indication		X			B.72
{ Replying IP-message indication }		X			B.73
Report origin authentication	X				B.74
{ Request for forwarding address }			X		B.75
Requested delivery method	X				B.76
Restricted delivery	X				B.77
Return of content	X				B.78

Secure access management	X				B.79
Sensitivity indication		X			B.80
Special delivery			X		B.81
Stored message alert				X	B.82
{ Stored message auto-forward }				X	B.83
Stored message deletion				X	B.84
Stored message fetching				X	B.85
Stored message listing				X	B.86
Stored message summary				X	B.87
Subject indication		X			B.88
{ Submission time stamp indication }	X				B.89
Type body		X			B.90
{ Undeliverable mail with return of physical message }			X		B.91
Use of distribution list	X				B.92
{ User/UA capabilities registration }	X				B.93

Tableau 3/F.400 [2T3.400], p. 19

19 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 4/F.400.

H.T. [T4.400]

TABLE 4/F.400
Elements of service belonging to the basic MT service

Elements of service	Annex B ref.
Access management	B.1
Content type indication	B.12
Converted indication	B.15
{	
Delivery time stamp indication	
}	B.22
Message indication	B.41
Non-delivery notification	B.47
{	
Original encoded information types indication	
}	B.54
{	
Submission time stamp indication	
}	B.89
{	
User/UA capabilities registration	
}	B.93

Table 4/F.400 [T4.400], p.

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 5/F.400 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 6/F.400-9/F.400.

H.T. [T5.400]

TABLE 5/F.400

MT service optional user facilities

Elements of service	Classification	Available	Annex B ref.
Alternate recipient allowed	E	PM	B.3
{			
Alternate recipient assignment			
}	A	CA	B.4
Content confidentiality	A	PM	B.10
Content integrity	A	PM	B.11
Conversion prohibition	E	PM	B.13
{			
Conversion prohibition in case of loss of information			
}	A	PM	B.14
Deffered delivery	E	PM	B.19
Defered delivery cancellation	E	PM	B.20
Delivery notification	E	PM	B.21
{			
Designation of recipient by directory name			
}	A	PM	B.24
{			
Disclosure of other recipients			
}	E	PM	B.25
{			
DL expansion history indication			
}	E	PM	B.26
DL expansion prohibited	A	PM	B.27
Explicit conversion	A	PM	B.30
Grade of delivery selection	E	PM	B.32
Hold for delivery	A	CA	B.33
Implicit conversion	A	CA	B.34
Lastest delivery designation	A	PM	B.39
Message flow confidentiality	A	PM	B.40
Message origin authentication	A	PM	B.42
Message security labelling	A	PM	B.43
Message sequence integrity	A	PM	B.44
Multi-destination delivery	A	PM	B.45
{			
Non-repudiation of delivery			
}	A	PM	B.49
{			
Non-repudiatation of origin			
}	A	PM	B.50
{			
Non-repudiation of submission			
}	A	PM	B.51
{			
Originator requested alternate recipient			
}	A	PM	B.56
{			
Prevention of non-delivery notification			
}	A	PM	B.61
Probe	E	PM	B.63
Probe origin authentication	A	PM	B.64
Proof of delivery	A	PM	B.65
Proof of submission	A	PM	B.66
{			
Redirection disallowed by originator			
}	A	PM	B.68
{			
Redirection of incoming messages			
}	A	CA	B.69
Report origin authentication	A	PM	B.74
Requested delivery method	E | ua)	PM	B.76
Restricted delivery	A	CA	B.77

Return of content	A	PM	B.78
Secure access management	A	CA	B.79
Use of distribution list	A	PM	B.92

a) Does not imply the provision of all delivery methods which may be requested.

Table 5/F.400 [T5.400], p.

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 6/F.400. When this intercommunication is provided, through a PDAU, all the elements of service shown in Table 6/F.400 shall be supported.

H.T. [T6.400]

TABLE 6/F.400

Elements of service belonging to the base MH/PD service intercommunication

Elements of service	Annex B ref.
Basic physical rendition	B.7
Ordinary mail	B.53
Physical forwarding allowed	B.59
{	
Undeliverable mail with return of physical message	
}	B.91

Table 6/F.400 [T6.400], p.

19.5 *Optional user facilities for MH/PD service intercommunication*

Base MH/PD elements of servie § 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 7/F.400.

H.T. [T7.400]

TABLE 7/F.400

Optional user facilities for MH/PD service intercommunication

Elements of service	Classification	Annex B ref.
Additional physical rendition	A	B.2
Counter collection	E	B.16
{ Counter collection with advice }	A	B.17
{ Delivery via Bureaufax service }	A	B.23
{ EMS (express mail service) | ua) }	E	B.28
{ Physical delivery notification by MHS }	A	B.57
{ Physical delivery notification by PDS }	A	B.58
{ Notification forwarding prohibited }	A	B.60
Registered mail	A	B.70
{ Registered mail to addressee in person }	A	B.71
{ Request for forwarding address }	A	B.75
Special delivery | ua)	E	B.81

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

Table 7/F.400 [T7.400], p.

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 8/F.400. When an MS is provided, all the elements of service shown in Table 8/F.400 shall be supported.

H.T. [T8.400]

TABLE 8/F.400

Base message store

Elements of service	**Annex B ref.**
Stored message deletion	**B.84**
Stored message fetching	**B.85**
Stored message listing	**B.86**
Stored message summary	**B.87**

Table 8/F.400 [T8.400], p.

19.7 *MS optional user facilities*

Base MS elements of service (§ 19.6) together with the optional user facilities listed below can be used together 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 9/F.400.

H.T. [T9.400]

TABLE 9/F.400

MS optional user facilities

Elements of service	Classification	Annex B ref.
Stored message alert	A	B.82
{		
Stored message auto-forward		
}	A	B.83

Table 9/F.400 [T9.400], p.

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 O/R 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 10/F.400.

H.T. [T10.400]

TABLE 10/F.400

Elements of service belonging to the basic IPM service

Elements of service	Annex B ref.
Access management	B.1
Content type indication	B.12
Converted indication	B.15
{ Delivery time stamp indication }	B.22
IP-message identification	B.37
Message identification	B.41
Non-delivery notification	B.47
{ Original encoded information types indication }	B.54
{ Submission time stamp indication }	B.89
Typed body	B.90
{ User/UA capabilities registration }	B.93

Table 10/F.400 [T10.400], p.

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 Table 11/F.400 and Table 12/F.400, 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.

Note — With the access protocol described in Recommendation T.330, teletex terminals are able to make use of the basic IPM service as well as of the optional user facilities provided by the message handling system.

H.T. [1T11.400]
TABLE 11/F.400
IPM optional user facilities selectable on a per-message basis

Elements of service	Origination	Reception	Annex B ref.
Additional physical rendition	A	A	B.2
Alternate recipient allowed	A	A	B.3
Authorizing users indication	A	E	B.5
Auto-forwarded indication	A	E	B.6
Basic physical rendition	A	E*	B.7
{ Blind copy recipient indication }	A	E	B.8
{ Body part encryption indication }	A	E	B.9
Content confidentiality	A	A	B.10
Content integrity	A	A	B.11
Conversion prohibition	E	E	B.13
{ Conversion prohibition in case of loss of information }		N/A	B.14
Counter collection	A	E*	B.16
{ Counter collection with advice }	A	A	B.17
{ Cross-referencing indication }	A	E	B.18
Deffered delivery	E	N/A	B.19
{ Deffered delivery cancellation }	A	N/A	B.20
Delivery notification	E	N/A	B.21
{ Delivery via Bureaufax service }	A	A	B.23
{ Designation of recipient by directory name }	A	N/A	B.24
{ Disclosure of other recipients }	A	E	B.25
{ DL expansion history indication }	N/A	E	B.26
DL expansion prohibited	A	A	B.27
{ EMS (express mail service) | ua) }	A	E*	B.28
Expiry date indication	A	E	B.29
Explicit conversion	A	N/A	B.30
{ Forwarded IP-message indication }	A	E	B.31
Grade of delivery selection	E	E	B.32
Importance indication	A	E	B.35
Incomplete copy indication	A	A	B.36
Language indication	A	E	B.38
Latest delivery designation	A	N/A	B.39
Message flow confidentiality	A	N/A	B.40
Message origin authentication	A	A	B.42
Message security labelling	A	A	B.43
Message sequence integrity	A	A	B.44
Multi-destination delivery	E	N/A	B.45
Multi-part body	A	E	B.46

{ Non-receipt notification request indication }	A	E	B.48
{ Non-repudiation of delivery }	A	A	B.49
Non-repudiation of origin	A	A	B.50
{ Non-repudiation of submission }	A	A	B.51
Obsoleting indication	A	E	B.52
Ordinary mail	A	E*	B.53
Originator indication	E	E	B.55
{ Originator requested alternate recipient }	A	N/A	B.56
{ Physical delivery notification by MHS }	A	A	B.57
{ Physical delivery notification by PDS }	A	E*	B.58
Physical forwarding allowed	A	E*	B.59

Tableau 11/F.400 [1T11.400], p. 27

H.T. [2T11.400]

TABLE 11/F.400 *(cont.)*

Elements of service	Origination	Reception	Annex B ref.
{ Physical forwarding prohibited }	A	E*	B.60
{ Prevention of non-delivery notification }	A	N/A	B.61
{ Primary and copy recipients indication }	E	E	B.62
Probe	A	N/A	B.63
Probe origin authentication	A	A	B.64
Proof of delivery	A	A	B.65
Proof of submission	A	A	B.66
{ Receipt notification request indication }	A	A	B.67
{ Redirection disallowed by originator }	A	N/A	B.68
Registred mail	A	A	B.70
{ Registred mail to addressee in person }	A	A	B.71
Reply request indication	A	E	B.72
{ Reply IP-message indication }	E	E	B.73
Report origin authentication	A	A	B.74
{ Request for forwarding address }	A	A	B.75
Requested delivery method	E	N/A	B.76
Return of content	A	N/A	B.78
Sensitivity indication	A	E	B.80
Special delivery | ua)	A	E*	B.81
Stored message deletion	N/A	E**	B.84
Stored message fetching	N/A	E**	B.85
Stored message listing	N/A	E**	B.86
Stored message summary	N/A	E**	B.87
Subject indication	E	E	B.88
{ Undeliverable mail with return of physical message }	A	E*	B.91
Use of distribution list	A	A	B.92
Essential optional user facility has to be provided.			
Essential optional user facility only applying to PDAUs.			
Essential optional user facility only applying to MSs.			
Additional optional user facility can be provided.			

N/A Not applicable.

a) 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 by A.

Tableau 11/F.400 [2T11.400], p. 28

BLANC

H.T. [T12.400]

TABLE 12/F.400

IPM optional user facilities agreed for a contractual period of time

Elements of service	Classification	Annex B ref.
{ Alternate recipient assignment }	A	B.4
Hold for delivery	A	B.33
Implicit conversion	A	B.34
{ Redirection of incoming messages }	A	B.69
Restricted delivery	A	B.77
Secure access management	A	B.79
Stored message alert	A	B.82
{ Stored message auto-forward }	A	B.83

Tableau 12/F.400 [T12.400], p. 29

BLANC

MONTAGE: Annexe A sur le reste de cette page