INTERNATIONAL TELECOMMUNICATION UNION

# CCITT

# F.400/X.400

THE INTERNATIONAL
TELEGRAPH AND TELEPHONE
CONSULTATIVE COMMITTEE

(11/1988)

SERIES F: NON-TELEPHONE TELECOMMUNICATION SERVICES

Message handling services

SERIES X: DATA NETWORKS AND OPEN SYSTEM COMMUNICATIONS

Message handling systems

# MESSAGE HANDLING SYSTEM AND SERVICE OVERVIEW

Reedition of CCITT Recommendation F.400/X.400
published in the Blue Book, Fascicle II.6 (1988)

## NOTES

1 CCITT Recommendation F.400/X.400 was published in Fascicle II.6 of the *Blue Book*. This file is an extract from the *Blue Book.* While the presentation and layout of the text might be slightly different from the *Blue Book* version, the contents of the file are identical to the *Blue Book* version and copyright conditions remain unchanged (see below).

2 In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

**Recommendation F.400**[1)]

## 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 Recommendation.

CONTENTS

*PART 1 – Introduction*

[1)] Recommandation X.400 is identical to F.400.

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.

TABLE 1/F.400

**Structure of MHS Recommendations**

| Name of Recommendation/Standard | Joint MHS | | Joint support | | CCITT only | |
|---|---|---|---|---|---|---|
| | CCITT | ISO | 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 | 9070-2 | | |

## 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 100213) |
| 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.

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.

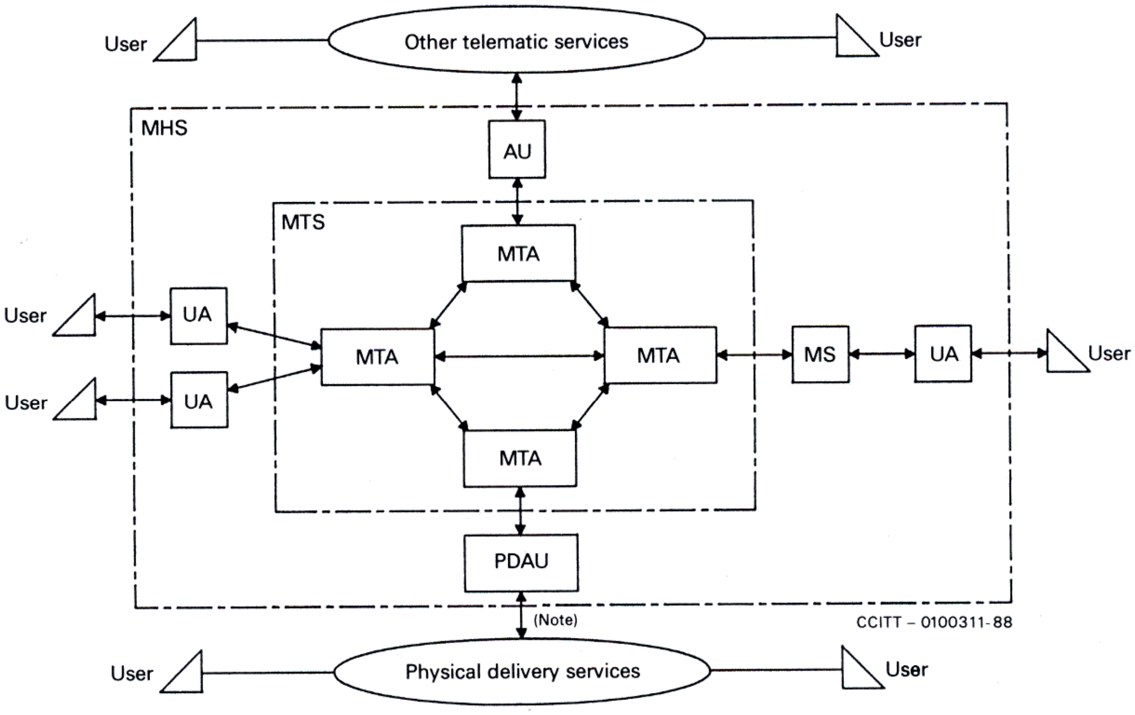
An originator prepares messages with the assistance of his user agent. A user agent (UA) is an application process that interacts with the message transfer system (MTS) or a message store (MS), to submit messages on behalf of a single user. The MTS delivers the messages submitted to it, to one or more 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).



*Note* – Message input from PD Services to MHS is for further study. Flow from PD Services to the PDAU shown is for notifications.

FIGURE 1/F.400

**MHS functional model**

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).

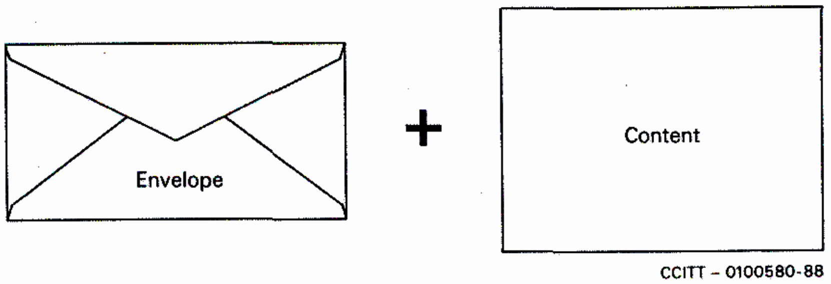


FIGURE 2/F.400

**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 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.

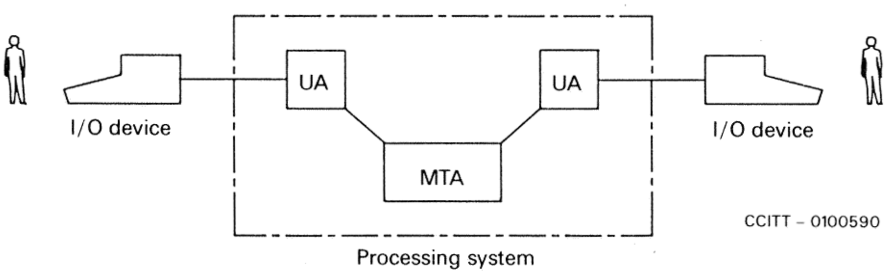


FIGURE 3/F.400

**Co-resident UA and MTA**

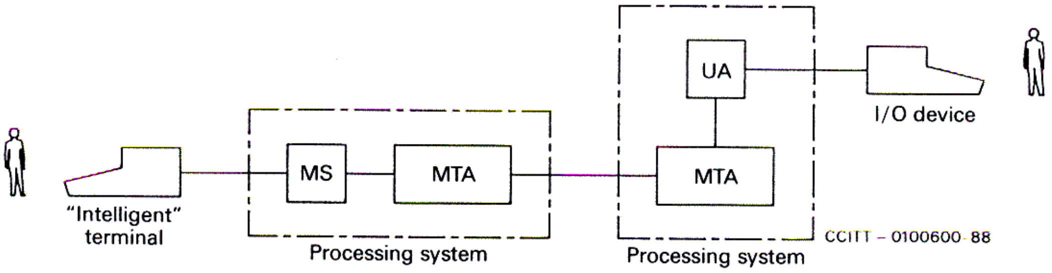


FIGURE 4/F.400

**Stand-alone UA and co-resident MS/MTA and US/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 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.

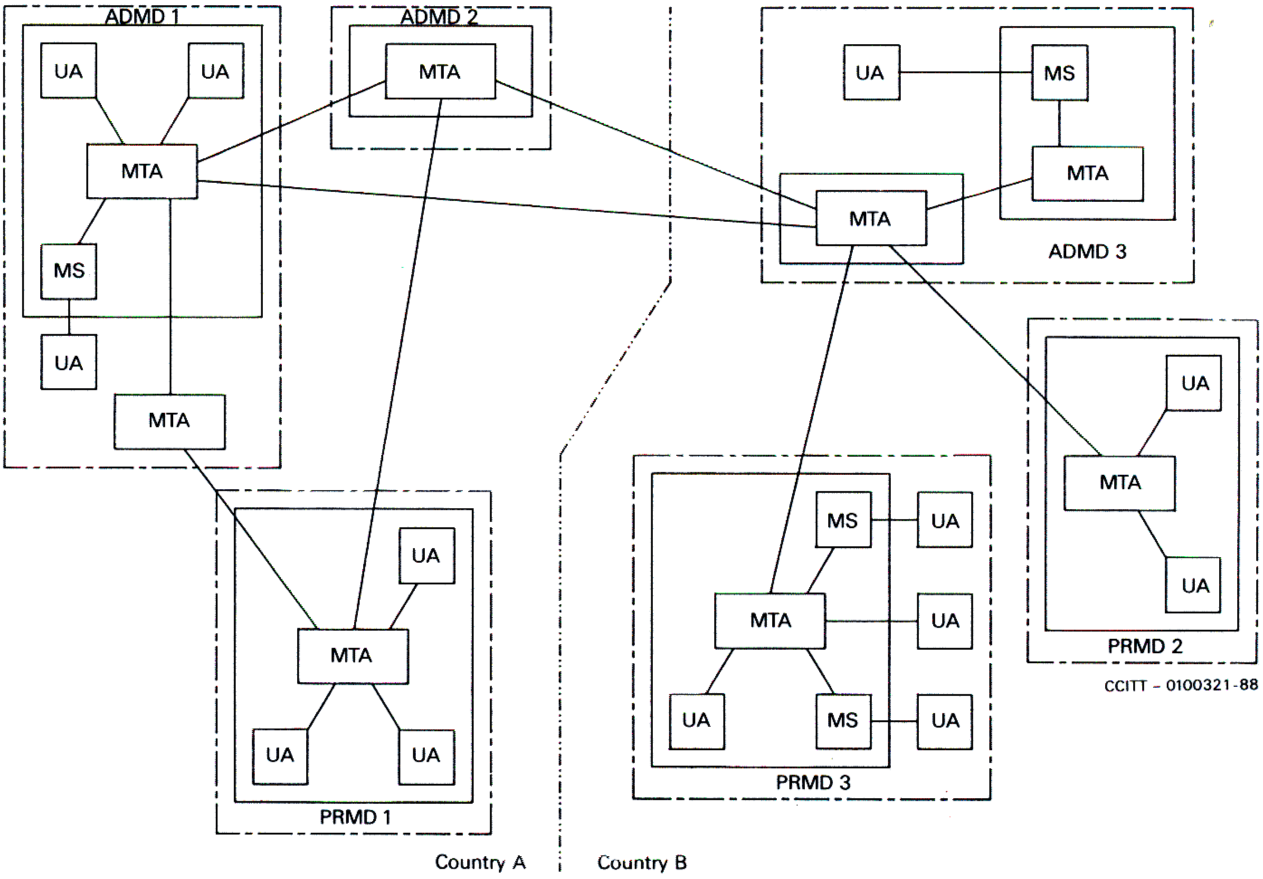


FIGURE 5/F.400

**Relationships between management domains**

*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.

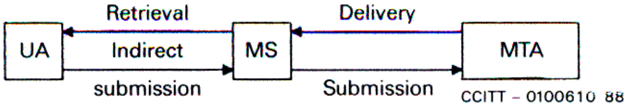


FIGURE 6/F.400

**Submission and delivery with an MS**

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.

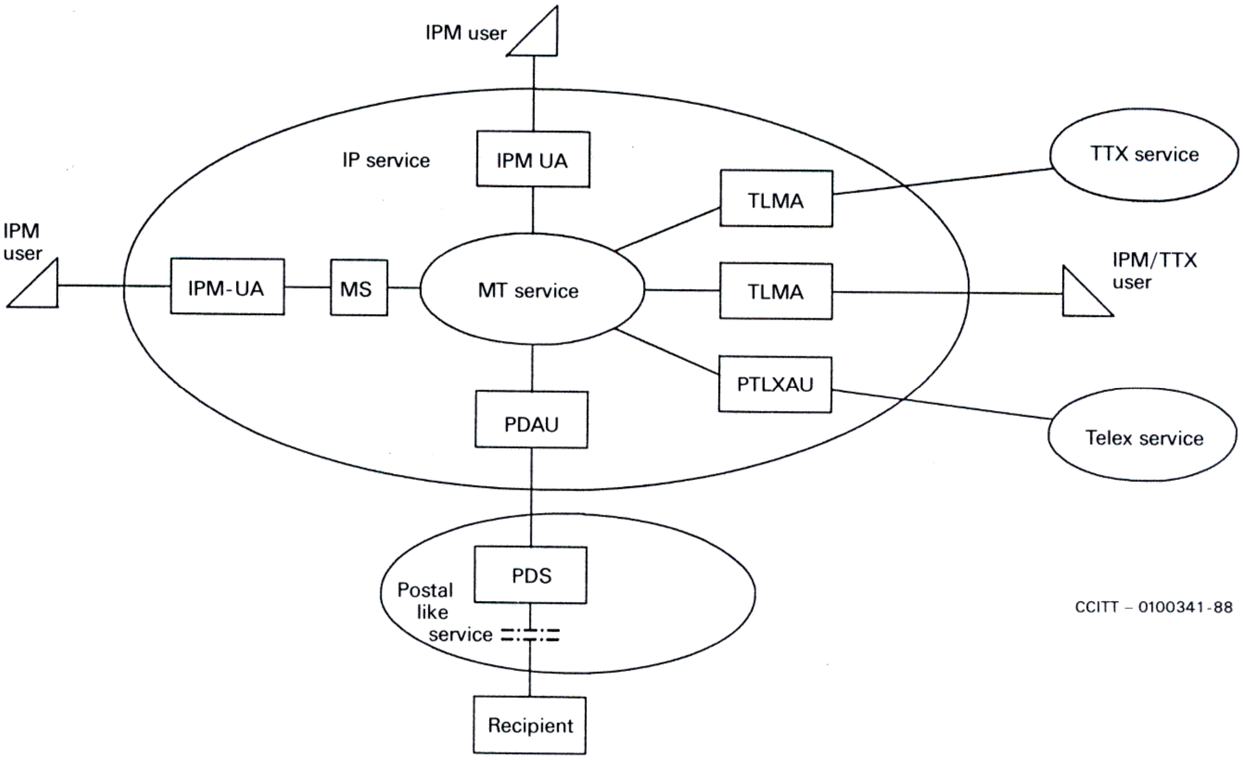


FIGURE 7/F.400

**IPM service functional model**

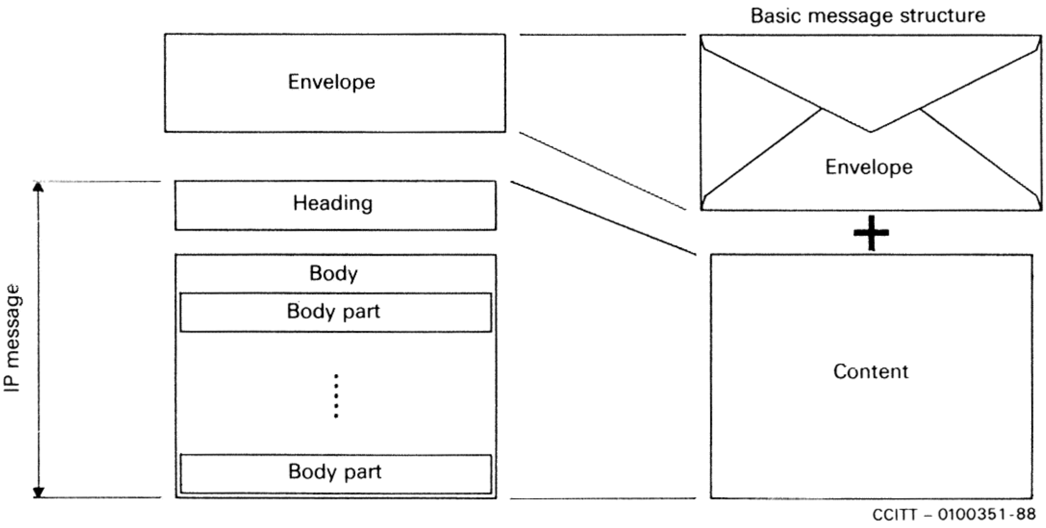
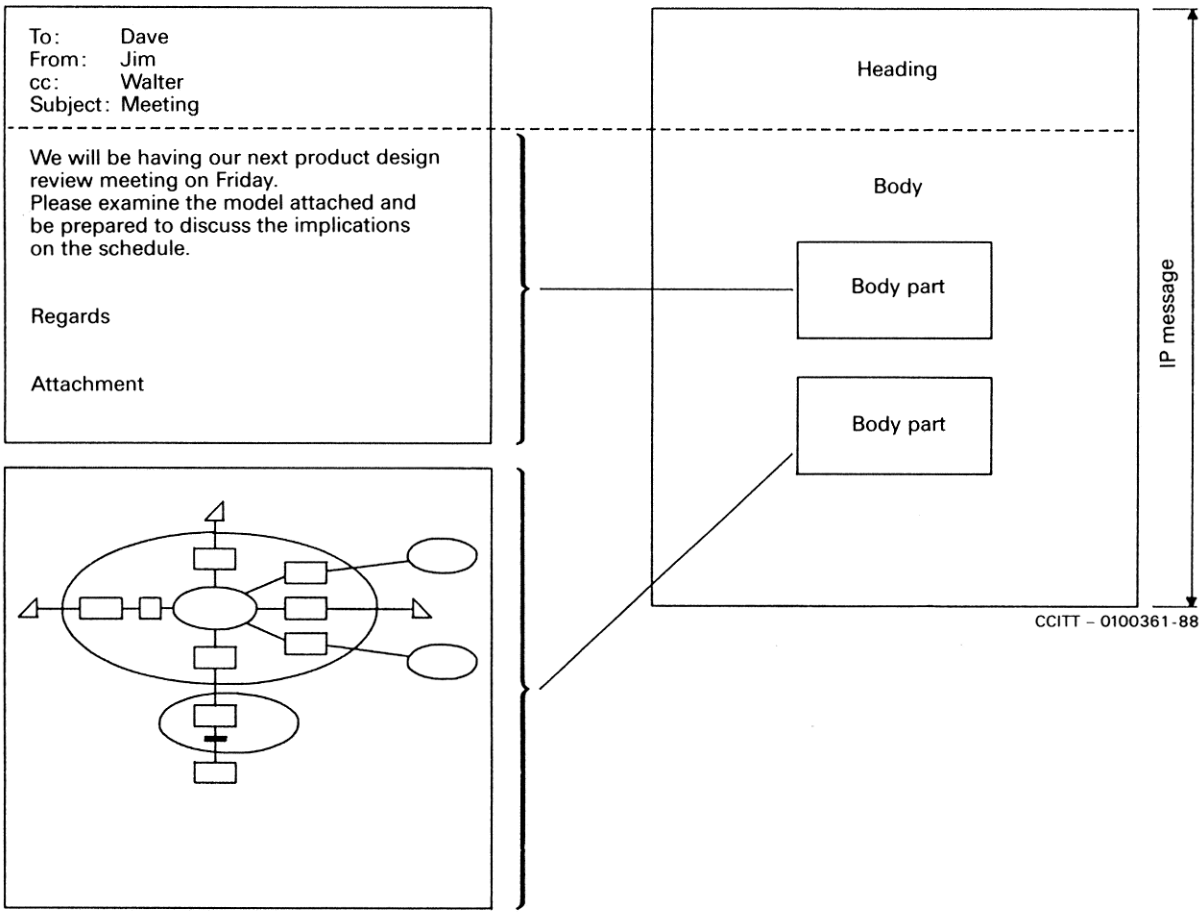


FIGURE 8/F.400

**IP-message structure**



To: Dave
From: Jim
cc: Walter
Subject: Meeting

We will be having our next product design review meeting on Friday. Please examine the model attached and be prepared to discuss the implications on the schedule.

Regards

Attachment

FIGURE 9/F.400
**IP-message structure for a typical memo**

### 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.

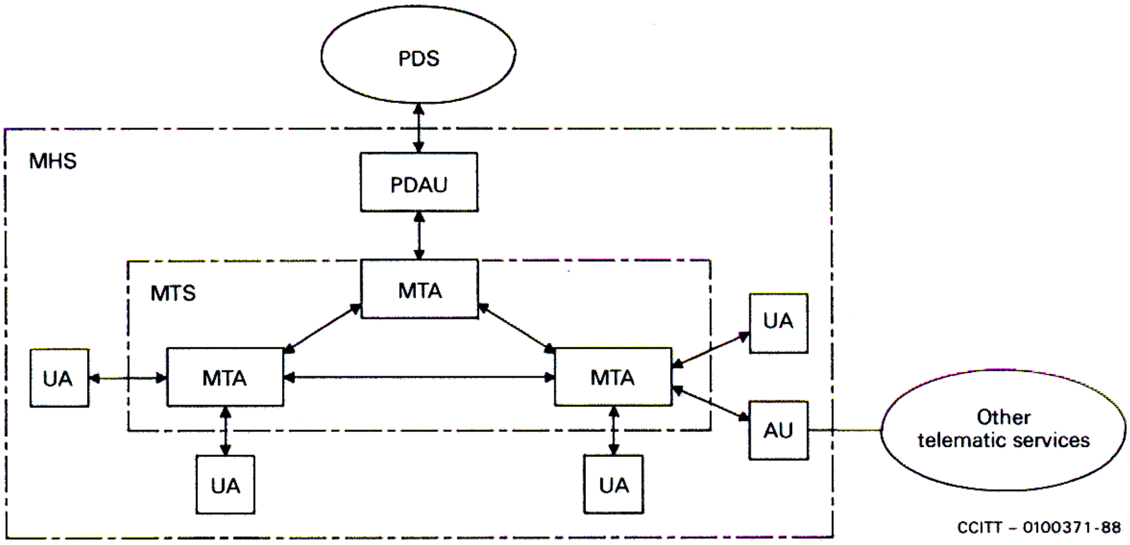


FIGURE 10/F.400

**Functional model MHS-PDS interworking**

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.

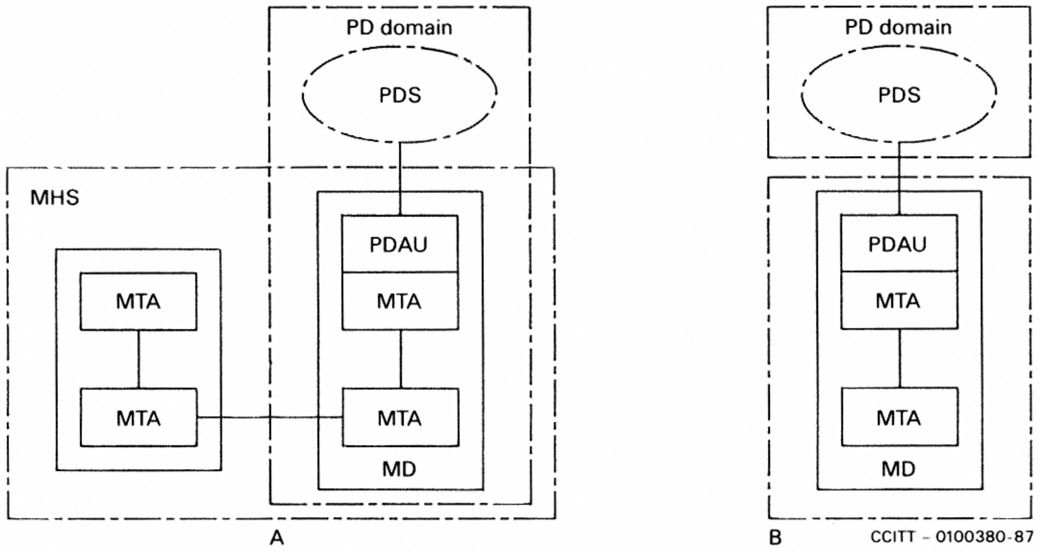


FIGURE 11/F.400

**Configurations for MH/'PD service intercommunication**

### 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.).

## 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.

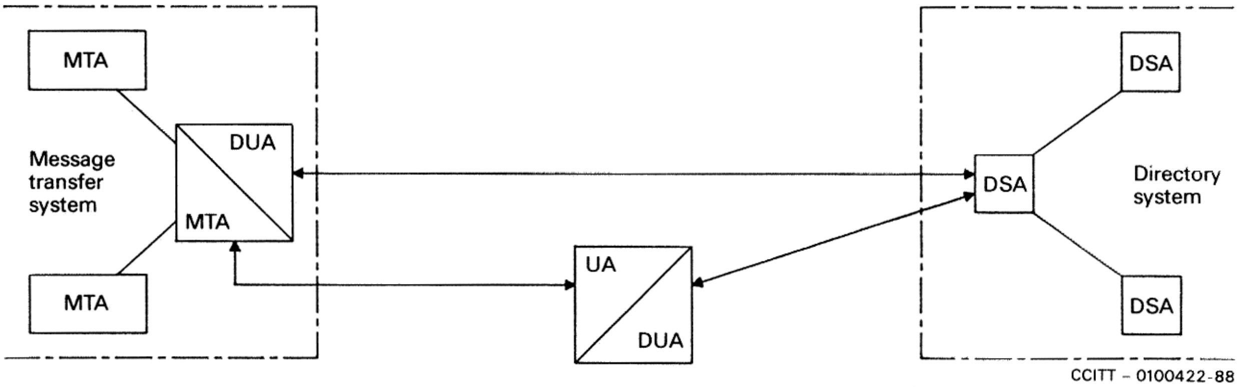


FIGURE 12/F.400

**Functional model on MHS-directory interworking**

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.

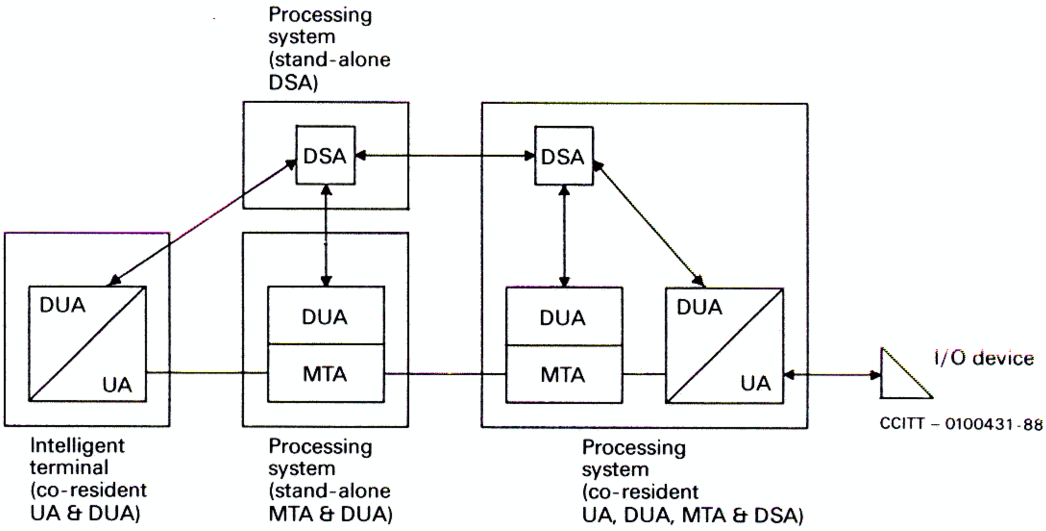

Processing system (stand-alone DSA)
DSA
DSA
DUA
UA
DUA
MTA
DUA
MTA
DUA
UA
I/O device
CCITT – 0100431-88
Intelligent terminal (co-resident UA & DUA)
Processing system (stand-alone MTA & DUA)
Processing system (co-resident UA, DUA, MTA & DSA)

FIGURE 13/F.400

**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 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.

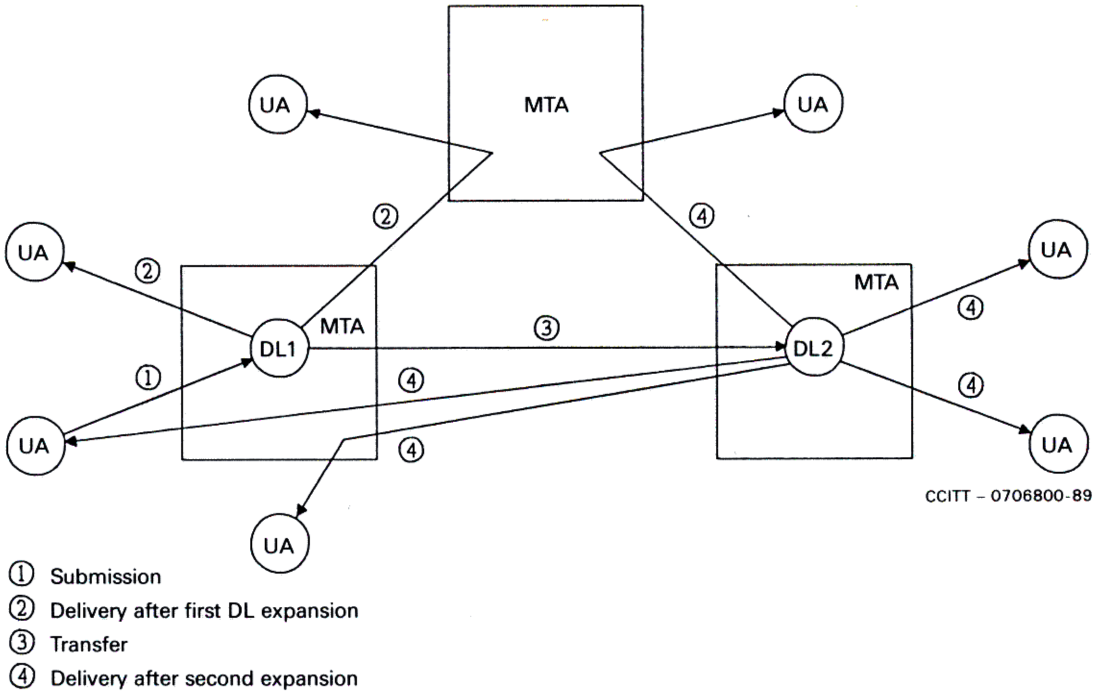


FIGURE 14/F.400

**Distribution list expansion**

### 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.

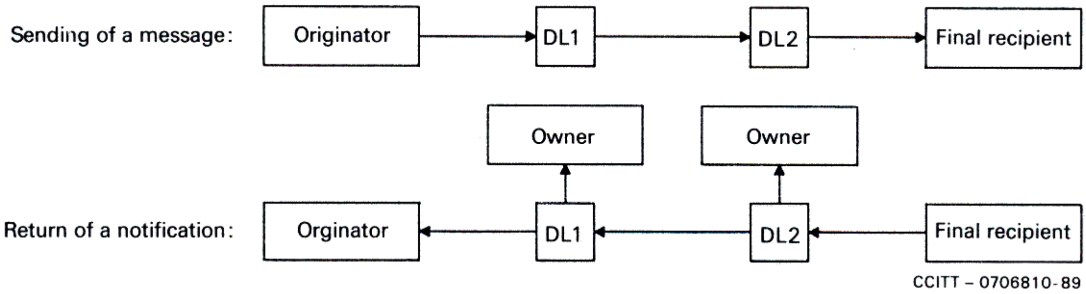


FIGURE 15/F.400

**DL notifications**

*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.

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 |

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 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.

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.

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 |
| Forwarded IP-message indication | | X | | | B.31 |
| Grade 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 |

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 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 forwarding 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 |

## 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.

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 |

### 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.

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 |
| Deferred delivery | E | PM | B.19 |
| Deferred 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 |
| Latest 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-repudiation 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[a)] | 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.

## 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.

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 |

## 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.

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)[a)] | 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 address in person | A | B.71 |
| Request for forwarding address | A | B.75 |
| Special delivery[a)] | E | B.81 |

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

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 |

### 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.

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 |

### 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.

TABLE 10/F.400

**Eléments de service appartenant au service MPP de base**

| 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 indentification | 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 |

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.

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 |
| Deferred delivery | E | N/A | B.19 |
| Deferred 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)[a)] | 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 |

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 |
| Registered mail | A | A | B.70 |
| Registered 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[a)] | 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 |

E Essential optional user facility has to be provided.

E* Essential optional user facility only applying to PDAUs.

E** Essential optional user facility only applying to MSs.

A 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.

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 |

## ANNEX A

(to Recommendation F.400)

## 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 X.400-Series Recommendations (especially X.402), where many entries are found. The terms have, depending on the source, varying levels of abstraction.

### A.1 **access unit (AU)**

*F: unité d'accés (UA)*

*S: unidad de acceso (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**

*F: destinataire effectif*

*S: destinatario real*

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

A.3 **administration**

*F: administration*

*S: administración*

In the context of CCITT an Administration (member of ITU) or a recognized private operating agency.

A.4 **administration domain name**

*F: nom d'un domaine d'administration*

*S: nombre de dominio de administración*

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)**

*F: domaine de gestion d'administration*

*S: dominio de gestión de administración*

A management domain that comprises messaging systems managed by an Administration.

A.6 **alternate recipient**

*F: destinataire suppléant*

*S: destinatario alternativo*

In the context of message handling a user or distribution list to which the originator can (but need not) request that a message or probe be conveyed if and only if it cannot be conveyed to a particular preferred recipient.

A.7 **attribute**

*F: attribut*

*S: atributo*

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**

*F: liste d'attributes*

*S: lista de atributos*

In the context of message handling, a data structure, an ordered set of attributes that constitutes an O/R address.

A.9 **attribute type**

*F: type d'attribut*

*S: tipo de atributo*

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

A.10 **attribute value**

*F: valeur d'attribut*

*S: valor de atributo*

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**

*F: service de base*

*S: servicio básico*

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

A.12 **body**

*F: corps*

*S: cuerpo*

Component of a message. Other components are the heading and the envelope.

A.13 **body part**

*F: partie du corps*

*S: parte del cuerpo*

Component of the body of a message.

A.14 **common name**

*F: nom courant*

*S: nombre común*

In the context of message handling, a standard attribute of an O/R 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**

*F: contenu*

*S: contenido*

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**

*F: type de contenu*

*S: tipo de contenido*

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

A.17 **conversion**

*F: conversion*

*S: conversión*

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**

*F: nom de pays*

*S: nombre de país*

In the context of message handling, a standard attribute of a name form that identifies a country. 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 (see also *physical delivery country name* and Recommendation F.415).

A.19 **delivery**

*F: remise*

*S: entrega*

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

A.20 **delivery report**

*F: rapport de remise*

*S: informe de entrega*

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**

*F: depôt direct*

*S: depósito directo*

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 **direct user**

*F: utilisateur direct*

*S: usuario directo*

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

A.23 **directory**

*F: annuaire*

*S: guía*

A collection of open systems cooperating to provide directory services.

A.24 **directory name**

*F: nom d'annuaire*

*S: nombre de guía*

Name of an entry in a directory.

*Note* – In the context of message handling, the entry in the directory will enable the O/R address to be retrieved for submission of a message.

A.25 **directory system agent (DSA)**

*F: agent de système d'annuaire (ASA)*

*S: agente de sistema de guía (ASG)*

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.26 **directory user agent (DUA)**

*F: agent d'usager d'annuaire (AUA)*

*S: agente de usuario de guía (AUG)*

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.27 **distribution list (DL)**

*F: liste de distribution (LD)*

*S: lista de distribución (LD)*

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 O/R names identifying either users or other distribution lists.

A.28 **distribution list expansion**

*F: allongement de liste de distribution*

*S: expansión de une lista de distribución*

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 **distibution list name**

*F: nom de liste de distribution*

*S: nombre de lista de distribución*

O/R name allocated to represent a collection of O/R addresses and directory names.

A.30 **domain**

*F: domaine*

*S: dominio*

See *management domain*.

A.31 **domain defined attributes**

*F: attributs définis d'un domaine*

*S: atributos definidos por el dominio*

Optional attributes of an O/R address allocated to names in the responsibility of a management domain.

A.32 **element of service**

*F: element de service*

*S: elemento de servicio*

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

A.33 **encoded information type (EIT)**

*F: type de codage (TC)*

*S: tipo de información codificada (TIC)*

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

A.34 **envelope**

*F: enveloppe*

*S: sobre*

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**

*F: conversion explicite*

*S: conversión explícita*

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**

*F: développement de composants d'adresse de remise physique*

*S: componentes de ampliación de dirección de entrega física*

Standard attribute of a postal O/R 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, or room and floor numbers in a large building.

A.37 **extension of postal O/R address components**

*F: développement de composants d'adresse postale E/D*

*S: componentes de ampliación de dirección postal O/D*

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

A.38 **formatted postal O/R address**

*F: adresse postale E/D formatée*

*S: dirección postal O/D formatizada*

O/R address based on a postal address with formatted attributes.

A.39 **heading**

*F: en-tête*

*S: encabezamiento*

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

A.40 **immediate recipient**

*F: destinataire direct*

*S: destinatario inmediato*

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.41 **implicit conversion**

*F: conversion implicite*

*S: conversión implícita*

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

A.42 **indirect submission**

*F: depôt indirect*

*S: depósito indirecto*

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.43 **indirect user**

*F: utilisateur indirect*

*S: usuario indirecto*

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.44 **intercommunication**

*F: intercommunication*

*S: intercomunicación*

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, the intercommunication between message handling services and physical delivery services.

A.45 **interpersonal messaging service**

*F: service de messagerie de personne à personne*

*S: servicio de mensajería interpersonal*

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.46 **IP-message**

*F: message IP*

*S: mensaje IP*

The content of a message in the IPM Service.

A.47 **local postal attributes**

*F: attributs postaux locaux*

*S: atributos postales locales*

Standard attributes of a post O/R 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.48 **management domain (MD)**

*F: domaine de gestion (DG)*

*S: dominio de gestión (DG)*

In the context of message handling, a set of messaging systems – at least one of which contains, or realizes, an MTA – at 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.49 **management domain name**

*F: nom d'un domaine de gestion*

*S: nombre de dominio de gestión*

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

A.50 **members**

*F: membres*

*S: miembros*

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

A.51 **message**

*F: message*

*S: mensaje*

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

A.52 **message handling (MH)**

*F: messagerie (traitement des mesages) (M)*

*S: tratamiento de mensaje (TM)*

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

A.53 **message handling environment**

*F: environnement de traitement de messages*

*S: entorno de tratamiento de mensajes*

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,

– access units,

– users.

A.54 **message handling service**

*F: service de messagerie*

*S: servicio de tratamiento de mensajes*

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.55 **message handling system (MHS)**

*F: système de messagerie (STM)*

*S: sistema de tratamiento de mensajes*

The functional object, a component of the message handling environment, that conveys information objects from one party to another.

A.56 **message storage**

*F: mémorisation des messages*

*S: almacenamiento de mensajes*

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

A.57 **message store (MS)**

*F: mémoire des messages (MM)*

*S: memoria de mensajes (MM); alamacenador de mensajes (AM)*

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

A.58 **message transfer (MT)**

*F: transfert de messages (TM)*

*S: transferencia de mensajes (TRM)*

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

A.59 **message transfer agent (MTA)**

*F: agent de transfert de messages (ATM)*

*S: agente de transferencia de mensajes (ATM)*

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

A.60 **message transfer service**

*F: service de transfert de messages*

*S: servicio de transferenicia de mensajes*

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

A.61 **message transfer system (MTS)**

*F: système de transfert de messages (système TM)*

*S: sistema de transferencia de mensajes (STRM)*

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.62 **messaging system**

*F: système de messagerie*

*S: sistema de mensajeria*

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.63 **mnemonic O/R address**

*F: adresse mnémonique E/D*

*S: dirección O/D nemotécnica*

An O/R address tha mnemonicly 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.64 **naming authority**

*F: autorité responsable de l'appellation*

*S: autoridad de denominación*

An authority responsible for the allocation of names.

A.65 **network address**

*F: adresse réseau*

*S: dirección de red*

In the context of message handling, a standard attribute of an O/R 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.66 **non-delivery**

*F: non-remise*

*S: no entrega*

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.67 **non-registered access**

*F: accès non homologué*

*S: acceso no registrado*

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 O/R address.

A.68 **numeric O/R address**

*F: adresse numérique E/D*

*S: dirección O/D numérica*

In the context of message handling, an O/R 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.69 **numeric user identifier**

*F: identificateur numérique d'utilisateur*

*S: identificador de usuario numérico*

Standard attribute of an O/R address as a unique sequence of numeric information for identifying a user.

A.70 **O/R address**

*F: adresse E/D*

*S: dirección O/D*

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.71 **O/R name**

*F: nom E/D*

*S: nombre O/D*

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 O/R name distinguishes one user or distribution list from another and can also identify its point of access to MHS.

A.72 **optional user facilities**

*F: services complémentaires offerts en option á l'utilisateur*

*S: faciladad facultativa de usuario*

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.73 **organization name**

*F: nom d'organisation*

*S: nombre de la organización*

Standard attribute of an O/R address as a unique designation of an organization for the purpose of sending and receiving of messages.

A.74 **oganizational unit name**

*F: nom d'une unité d'organisation*

*S: nombre de la unidad organizacional*

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

A.75 **originator**

*F: expediteur*

*S: originador*

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

A.76 **personal name**

*F: nom personnel*

*S: nombre personal*

In the context of message handling, a standard attribute of an O/R 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.77 **physical delivery (PD)**

*F: remise physique (RP)*

*S: entrega física (EF)*

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

A.78 **physical delivery access unit (PDAU)**

*F: unité d'accès de remise physique (UARP)*

*S: unidad de acceso de entrega fisica (UAEF)*

An access unit that subjects messages (but neither probes nor reports) to physical rendition.

A.79 **physical delivery address components**

*F: composants d'une adresse de remise physique*

*S: componentes de dirección de entrega física*

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 components”.

A.80 **physical delivery country name**

*F: nom du pays de remise physique*

*S: nombre de país de entrega física*

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

A.81 **physical delivery domain**

*F: domaine de remise physique*

*S: dominio de entrega física*

The domain of responsibility of an organization providing a physical delivery system and optionally an MTA/PDAU.

A.82 **physical delivery office address components**

*F: composants d'une adresse de bureau de remise physique*

*S: componentes de dirección de oficina de entrega física*

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.83 **physical delivery office name**

*F: nom du bureau de remise physique*

*S: nombre de oficina de entrega fisica*

Standard attribute of a postal O/R 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.84 **physical delivery office number**

*F: numéro du bureau de remise physique*

*S: número de oficina de entrega física*

Standard attribute and in a postal O/R address a means to distinguish between more than one physical delivery office within a city etc.

A.85 **physical delivery organization name**

*F: nom d'organisation de remise physique*

*S: nombre de la organización de entrega física*

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

A.86 **physical delivery personal name**

*F: nom personnel de remise physique*

*S: nombre personal de entrega física*

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.87 **physical delivery service**

*F: service de remise physique*

*S: servicio de entrega física*

Service provided by a physical delivery system.

A.88 **physical delivery service name**

*F: nom du service de remise physique*

*S: nombre del servicio de entrega física*

Standard attribute of a postal O/R 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.89 **physical delivery system (PDS)**

*F: système de remise physique (SRP)*

*S: sistema de entrega física (SEF)*

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

A.90 **physical message**

*F: message physique*

*S: mensaje físico*

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

A.91 **physical rendition**

*F: conversion physique*

*S: reproducción física*

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.92 **postal code**

*F: code postal*

*S: código postal*

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

A.93 **postal O/R address**

*F: adresse postale E/D*

*S: dirección postal O/D*

In the context of message handling, an O/R address that identifies a user by means of its postal address. It identifies the physical delivery system through which the user is to access and gives the user's postal address.

A.94 **postal O/R address components**

*F: composants d'une adresse postale E/D*

*S: componentes de dirección postal O/D*

They contain in a postal address information to decribe the sender or addressee by means of his name (physical delivery personal name, physical delivery 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 O/R address components".

A.95 **post office box address (P.O. box address)**

*F: unité d'accés de remise physique (UARP)*

*S: unidad de acceso de entrega física (UAEF)*

An access unit that subjects messages (but neither probes nor reports) to physical rendition.

A.96 **post restante address**

*F: adresse poste restante*

*S: dirección lista de correos*

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

A.97 **potential recipient**

*F: destinataire potential*

*S: destinatario potencial*

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

A.98 **preferred recipient**

*F: destinataire preféré*

*S: receptor preferido*

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

A.99 **private domain name**

*F: nom d'un domain privé*

*S: nombre de dominio privado*

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

*Note* – They are administered by the ADMD the PRMD is associated with.

A.100 **private management domain (PRMD)**

*F: domaine de gestion privé (DGPR)*

*S: dominio de gestión privado*

In the context of message handling, a management domain that comprises messaging system(s) managed by an organization other than an Administration.

A.101 **probe**

*F: essai*

*S: sonda*

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 message and that is used to determine the deliverability of such messages.

A.102 **public message handling service**

*F: service public de messagerie*

*S: servicio público de tratamiento de mensajes*

Message handling service offered by an Administration.

A.103 **public services**

*F: services publics*

*S: servicios públicos*

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

A.104 **receipt**

*F: réception*

*S: recepción*

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.105 **recipient**

*F: destinataire*

*S: destinatario*

See *actual recipient*.

A.106 **recursion**

*F: récursivité*

*S: repetición*

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.107 **redirection**

*F: réacheminement*

*S: redireccionamiento*

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.108 **registered access**

*F: accès homologué*

*S: acceso registrado*

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 O/R address.

A.109 **report**

*F: rapport*

*S: informe*

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.110 **retrieval**

*F: extraction*

*S: recuperación*

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.111 **security capabilities**

*F: capacité de sécurité*

*S: capacidades de seguridad*

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

A.112 **specialized access**

*F: accès spécialisé*

*S: acceso especializado*

In the context of message handling, the involvement of specialized access units providing intercommunication between message handling services and other telecommunication services.

A.113 **standard attribute**

*F: attribut normalisé*

*S: atributo normalizado*

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

A.114 **street address**

*F: adresse de rue*

*S: dirección-calle*

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.115 **subject**

*F: objet*

*S: asunto*

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.116 **subject message**

*F: message objet*

*S: mensaje de asunto*

The message that is the subject of a report.

A.117 **subject probe**

*F: essai objet*

*S: sonda de asunto*

The probe that is the subject of a report.

A.118 **submission**

*F: dépôt*

*S: depósito*

Direct submission or indirect submission.

A.119 **substitute recipient**

*F: destinataire substitut*

*S: destinatario sustituto*

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

A.120 **terminal identifier**

*F: identificateur de terminal*

*S: identificador de terminal*

Standard attribute in an O/R address providing information for identifying a terminal amongst others.

*Note* – Examples are telex answerback and teletex terminal identifier.

A.121 **terminal O/R address**

*F: adresse terminale E/D*

*S: dirección O/D de terminal*

In the context of message handling, an O/R 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.122 **terminal type**

*F: type de terminal*

*S: tipo de terminal*

Standard attribute of an O/R address that indicates the type of a terminal.

*Note* – Examples: telex, teletex, G3 facsimile, G4 facsimile, IA5, videotex terminal.

A.123 **transfer**

*F: transfert*

*S: transferencia*

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

A.124 **transfer system**

*F: système de transfert*

*S: sistema de transferencia*

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

A.125 **transmittal**

*F: transmission*

*S: transmisión*

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, or any report it provokes. It is a sequence of transmittal steps and events.

A.126 **unformatted postal O/R address**

*F: adresse postale E/D non formatée*

*S: dirección postal O/D no formatizada*

O/R address based on an unformatted postal address.

A.127 **unique postal name**

*F: nom postal unique*

*S: nombre postal exclusivo*

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.128 **user**

*F: usager/utilisateur*

*S: usuario*

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.129 **user agent (UA)**

*F: agent d'usager (AU)*

*S: agente de usuario (AU)*

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.

Component of MHS the user interacts with.

## ANNEX B

(to Recommendation F.400)

## Definitions of elements of service

*Note* – The abbreviations used in the title lines have the following meanings:

| | |
|---|---|
| TM | Message transfer |
| IPM | Interpersonal messaging |
| PD | Physical delivery |
| MS | Message store |
| PR | Per recipient (available on a per-recipient basis) |

### B.1 *Access management* TM

This element of service enables a UA and 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 O/R 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 renditon facilities (e.g., kind of paper, colour 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 submmitted 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 assinged to receive such messages. This UA will be notified of the O/R 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 orginization 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 *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.6 *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-31) 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.7 *Basic physical rendition* PD PR

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

B.8 *Blind copy recipient indication* IPM PR

This element of service allows the originator to provide the O/R 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.9 *Body part encryption indication* IPM

This element of service allows the originator to indicate to the recipient that a particular body 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. This element of service, however, does not itself encrypt or decrypt any body part.

B.10 *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.11 *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.12 *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 cooperating UAs.

B.13 *Conversion prohibition* MT

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

B.14 *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) should 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 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.15 *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.16 *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.17 *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, or teletex, using the number provided by the originator.

B.18 *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.19 *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 data 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.

*Note* – Storage of the message shall be handled in the originating country.

### B.20 *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.21 *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 access unit. The notification is related to the submitted message by means of the message indentifier 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 or 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 content, has taken place.

### B.22 *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.23 *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.24 *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 O/R address.

### B.25 *Disclosure of other recipients* MT

This element of service enables the originating UA to instruct the MTS then submitting a multi-recipient message, to disclose the O/R names of all other recipients to each recipient UA, upon delivery of the message. The O/R 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.26 *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.27 *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.28 *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.29 *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.30 *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.31 *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 a IP-message.

### B.32 *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.33 *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.34 *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.35 *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.36 *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.37 *IP-message identification* IPM

This element of service enables cooperating IMP UAs to convey a globally unique identifier for each IP-message sent or received. The IP-message identifier is composed of an O/R 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.38 *Language indication* IPM

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

### B.39 *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.40 *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.41 *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.42 *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.43 *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.44 *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.45 *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.46 *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.

B.47 *Non-delivery notification* MT PR

This element of service enables the MTS to notify an originating UA if a submitted message was not delivered to the specified recipient UA(s). The reason the message was not deliverd is included as part of the notification. For example, the recipient UA can be unknown to the MTS.

In the case of a multi-destination message, a non-delivery notification can refer to any or all of the recipient UAs to which the message could not be delivered.

When a message is not 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.

B.48 *Non-receipt notification request indication* IPM PR

This element of service allows the originator to ask that he be notified should the IP-message be deemed unreceivable. In the case of a multi-recipient IP-message, the originator can request this element of service on a per-recipient basis.

The originator's UA conveys his request to the recipient's UA. The recipient's UA automatically issues a non-recipient notification when any of the following events occur:

1) the recipient's UA auto-forwards the IP-message to another user;

2) the recipient's UA discards the IP-message prior to receipt;

3) the recipient's subscription is terminated before he receives the IP-message.

Since receipt can occur arbitrarily long after delivery, the recipient's failure to access the IP-message, even for a long period of time (for example, while on an extended business trip), does not constitute non-receipt and thus no notification is issued.

*Note* – No legal significance can be adduced from this element of service.

B.49 *Non-repudiation of delivery* MT PR

This element of service allows the originator of a message to obtain from the recipient(s) of the message irrevocable proof that the message was delivered to the recipient(s). This will protect against any attempt by the recipient(s) to subsequently deny receiving the message or its content. Non-repudiation of delivery is provided to the originator of a message on a per-recipient basis using asymmetric encryption techniques.

B.50 *Non-repudiation of origin* MT PR

This element of service allows the originator of a message to provide the recipient(s) of the message irrevocable proof of the origin of the message. This will protect against any attempt by the originator to subsequently revoke the message or its content. Non-repudiation of origin is provided to the recipient(s) of a message on a per-message basis using asymmetric encryption techniques.

B.51 *Non-repudiation of submission* MT

This element of service allows the originator of a message to obtain irrevocable proof that a message was submitted to the MTS for delivery to the originally specified recipient(s). This will protect against any attempt by the MTS to subsequently deny that the message was submitted for delivery to the originally specified recipient(s). Non-repudiation of submission is provided to the originator of a message on a per-message basis, and uses an asymmetric encryption technique.

B.52 *Obsoleting indication* IPM

This element of service allows the originator to indicate to the recipient that one or more IP-messages he sent previously are obsolete. The IP-message that carries this indication supersedes the obsolete IP-message.

The action to be taken by the recipient or his IPM UA is a local matter. The intent, however, is to allow the IPM UA or the recipient to, for example, remove or file obsolete messages.

B.53 *Ordinary mail* PD PR

This element of service enables the PDS to transport and deliver the letter produced from the MHS message in the mode available through the ordinary letter mail service in the country of destination. This is the default action for the transport and delivery of a physical message.

B.54 *Original encoded information types indication* MT

This element of service enables an originating UA to specify to the MTS the encoded information types of a message being submitted. When the message is delivered, it also indicates to the recipient UA the encoded information types of the message specified by the originating UA.

B.55 *Orinigator indication* IPM

This element of service allows the identity of the originator to be conveyed to the recipient. The intent of this IPM element of service is to identify the originator in a user-friendly way. In contrast, the MTS provides to the recipient the actual O/R address and directory name, if present, of the originator. DL names should not be used in originator indication.

B.56 *Originator requested alternate recipient* M TPR

This element of service enables an originating UA to specify, for each intended recipient, one alternate recipient to which the MTS can deliver the message, if delivery to the intended recipient is not possible. The alternate recipient can be a distribution list. For the purposes of determining success or failure (and hence delivery and non-delivery notifications), delivery to the originator requested alternate recipient is equivalent to delivery to the intended recipient. If the intended recipient has requested redirection of incoming messages, and if the originating UA has requested redirection allowed by the originator, the system first tries to redirect the message. If this fails, the system then attempts to deliver the message to the designated alternate recipient.

B.57 *Physical delivery notification by MHS* PD PR

This element of service allows an originating user to request that an explicit notification, informing the originator of either successful or unsuccessful delivery of the physical message, be generated and returned by MHS. The notification provides information on delivery but no physical record is provided by the PDS.

*Note 1* – The notification includes the date and time of delivery based on the delivery confirmation given by the delivery person, the addressee or another authorized person. This is subject to national regulations in the destination contry and is also dependent on the type of delivery requested (e.g., in the case of registered mail to addressee in person, the addressee would be the confirming person).

*Note 2* – This notification carries no implication that any action on the part of the recipient (such as examination of the message content) has taken place.

*Note 3* – When this element of service is requested, and the physical message is undeliverable, it is either returned or destroyed depending on national regulations in the destination country, which means that the default action of the element of service B.91 is overridden.

B.58 *Physical delivery notification by PDS* PD PR

This element of service allows an originating user to request that an explicit notification, informing the originator of either successful or unsuccessful delivery of the physical message, be generated and returned by the PDS. The notification serves as a record of delivery for the originating user to retain for reference.

*Note 1* – The notification includes the date and time, and, in the case of successful delivery, the signature of the person confirming the delivery. The confirming person can be the delivery person, the addressee or another authorized person. This is subject to national regulations in the destination country and is also dependent on the type of delivery requested (e.g., in the case of registered mail to addressee in person, the addressee would be the confirming person).

*Note 2* – This notification carries no implication that any action on the part of the recipient (such as examination of the message content) has taken place.

*Note 3* – When this element of service is requested, and the physical message is undeliverable, is either returned or destroyed depending on national regulations in the destination country, which means that the default action of the element of service B.91 is overridden.

B.59 *Physical forwarding allowed* PD PR

This element of service enables the PDS to forward the physical message to a forwarding address if the recipient has changed his address and indicated this to the PDS. This is the default action taken by the PDS.

B.60 *Physical forwarding prohibited* PD PR

This element of service allows an originating user to instruct the PDS not to forward the physical message to a forwarding address.

B.61 *Prevention of non-delivery notification* MT PR

This element of service enables an originating UA to instruct the MTS not to return a non-delivery notification to the originating UA in the event that the message being submitted is judged undeliverable. In the case of a multi-destination message, the originating UA can request this element of service on a per-recipient basis.

B.62 *Primary and copy recipients indication* IPM

This element of service allows the originator to provide the names of zero or more users, or DLs, who are the intended primary recipients of the IP-message, and the names of zero or more users, or DLs, who are the intended copy recipients of the IP-message. It is intended to enable a recipient to determine the category in which each of the specified recipients (including the recipient himself) was placed. The exact distinction between these two categories of recipients is unspecified. However, the primary recipients, for example, might be expected to act upon the IP-message, while the copy recipients might be sent the IP-message for information only.

*Note* – As an example of this element of service in a typical memorandum, the primary recipients are normally designated by the directive “to:” while “cc:” identifies the copy recipients.

B.63 *Probe* MT

This element of service enables a UA to establish before submission whether a particular message could be delivered. The MTS provides the submission information and generates delivery and/or non-delivery notifications indicating whether a message with the same submission information could be delivered to the specified recipient UAs.

The probe element of service includes the capability of checking whether the content size, content type, and/or encoded information types would render it undeliverable. The significance of the result of a probe depends upon the recipient UA(s) having registered with the MTS the encoded information types, content type and maximum message size that it can accept. This element of service is subject to the same delivery time targets as for the urgent class. In the case of DLs, a probe indicates nothing about the likelihood of successful delivery to the DL members, but only whether the originator has the right to submit to the DL.

B.64 *Probe origin authentication* MT

This element of service allows the originator of a probe to provide to any MTA through which the probe is transferred a means to authenticate the origin of the probe (i.e. a signature). Probe origin authentication is on a per-probe basis, and uses an asymmetric encryption technique.

B.65 *Proof of delivery* MT PR

This element of service allows the originator of a message to obtain from the recipient(s) of the message the means to authenticate the identity of the recipient(s) and the delivered message and content. Message recipient authentication is provided to the originator of a message on a per-recipient basis using either symmetric or asymmetric encryption techniques.

B.66 *Proof of submission* MT

This element of service allows the originator of a message to obtain from the MTS the means to authenticate that the message was submitted for delivery to the originally intended recipient. Message submission authentication is provided on a per-message basis, and can use symmetric or asymmetric encryption techniques.

B.67 *Receipt notification request indication* IPM PR

This element of service allows the originator to ask that he be notified when the IP-message being sent is received. In the case of a multi-recipient message, the originator can request this element of service on a per-recipient basis. This element of service also implicitly requests non-receipt notification request indication.

The originator's UA conveys his request to the recipient's UA. The recipient can instruct his UA to honour such requests, either automatically (for example, when it first renders the IP-message on the recipient's terminal) or upon his explicit command. The recipient can also instruct his UA, either in blanket fashion or case by case, to ignore such requests.

B.68 *Redirection disallowed by originator* MT

This element of service enables an originating UA to instruct the MTS, if the recipient has requested the redirection of incoming messages element of service, that redirection should not be applied to a particular submitted message.

B.69 *Redirection of incoming messages* MT

This element of service enables a UA to instruct the MTS to redirect incoming messages addressed to it, to another UA or to a DL, for a specified period of time, or until revoked.

*Note 1* – This is an MT element of service that does not necessitate delivery to the intended recipient before redirection can take place. It is therefore distinct from the IPM Auto-Forwarded Indication Element of Service.

*Note 2* – When security provisions are in force, different incoming messages, on the basis of their security labels, may be redirected to separate alternate recipients or not re-directed at all.

B.70 *Registered mail* PD PR

This element of service allows an originating user to instruct the PDS to handle the physical message as registered mail.

B.71 *Registered mail to addressee in person* PD PR

This element of service allows an originating user to instruct the PDS to handle the physical message as registered mail and to deliver it to the addressee only.

B.72 *Reply request indication* IPM PR

This element of service allows the originator to request that a recipient send an IP-message in reply to the IP-message that carries the request. The originator can also specify the date by which any reply should be sent, and the one or more users and DLs to whom the originator requests (but does not demand) be among the preferred recipients of any reply. The recipient is informed of the date and names but it is up to the recipient to decide whether or not, and if so, to whom to reply.

*Note* – A blind copy recipient should consider carefully to whom he sends a reply, in order that the meaning of the blind copy recipient indication element of service is preserved.

B.73 *Replying IP-message indication* IPM

This element of service allows the originator of an IP-message to indicate to the recipient(s) that this IP-message is being sent in reply to another IP-message. A reply can, depending on the wishes of the originator of the replied-to message, and the final decision of the originator of the reply, be sent to:

1) the recipients specified in the reply request indication of the replied-to message;
2) the originator of the replied-to message;
3) the originator and other recipients;
4) a distribution list, in which the originator of the replied-to message can be a receiving member;
5) other recipients as chosen by the originator of the reply.

The recipients of the reply receive it as a regular IP-message, together with an indication of which IP-message it is a reply to.

B.74 *Report origin authentication* MT

This element of service allows the originator of a message (or probe) to authenticate the origin of a report on the delivery or non-delivery of the subject message (or probe), (a signature). Report origin authentication is on a per-report basis, and uses an asymmetric encryption technique.

B.75 *Request for forwarding address* PD PR

This element of service allows an originating user to instruct the PDS to provide the forwarding address if the recipient has changed his address and indicated this to the PDS.

This element of service can be used with either physical forwarding allowed or prohibited. The provision of the forwarding address by the PDS to an originating user is subject to national regulations in the destination country. The default action is no provision of the forwarding address.

B.76 *Requested delivery method* MT PR

This element of service allows a user to request, on a per-recipient basis, the preference of method or methods of message delivery (such as through an access unit). Non-delivery results if preference(s) cannot be satisfied.

B.77 *Restricted delivery* MT

This element of service enables a recipient UA to indicate to the MTS that it is not prepared to accept delivery of messages from certain originating UAs or DLs.

*Note 1* – This element of service can be requested in either of two ways:

a) specification by the recipient UA of unauthorized originators, all other originators are considered as authorized;

b) specification by the recipient UA of authorized originators, all other originators are considered to be unauthorized.

*Note 2* – The MTS abstract service specified in Rec. X.411 does not provide a technical realization of this element of service. Its provision may be the subject of further standardization.

B.78 *Return of content* MT

This element of service enables an originating UA to request that the content of a submitted message be returned with any non-delivery notification. This will not be done, however, if any encoded information type conversion has been performed on the message's content.

B.79 *Secure access management* MT

This element of service enables an MTS user to establish an association with the MTS, or the MTS to establish an association with an MTS user, or an MTA to establish an association with another MTA. It also establishes the strong credentials of the objects to interact, and the context and security-context of the association. Secure access management can use either an asymmetric or a symmetric encryption technique. When access security is achieved through strong credentials, they can be periodically updated.

B.80 *Sensitivity indication* IPM

This element of service allows the originator of an IP-message to specify guidelines for the relative sensitivity of the message upon its receipt. It is the intent that the sensitivity indication should control such items as:

1) whether the recipient should have to prove his identity to receive the IP-message;

2) whether the IP-message should be allowed to be printed on a shared printer;

3) whether an IPM UA should allow the recipient to forward the received IP-message;

4) whether the IP-message should be allowed to be auto-forwarded.

The sensitivity indication can be indicated to the recipient or interpreted directly by the recipient's IPM UA.

If no sensitivity level is indicated, it should be assumed that the IP-message originator has advised no restriction on the recipient's further disposition of the IP-message. The recipient is free to forward, print, or otherwise do as he chooses with the IP-message.

Three specific levels of sensitivity above the default are defined:

– *Personal*: The IP-message is sent to the recipient as an individual, rather than to him in his role. There is no implication that the IP-message is private, however.

– *Private*: The IP-message contains information that should be seen (or heard) only by the recipient, and not by anyone else. The recipient's IPM UA can provide services to enforce this intent on behalf of the IP-message originator.

– *Company-confidential*: The IP-message contains information that should be treated according to company-specific procedures.

B.81 *Special delivery* PD PR

This element of service allows an originating user to instruct the PDS to transport the letter produced form the MHS message through the ordinary letter mail circulation system and to deliver it by special messenger delivery.

B.82 *Stored message alert* MS

This element of service allows a user of an MS to register relevant sets of criteria that can cause an alert to be generated to the user when a message arrives at the MS satisfying the selected criteria. The generation of the alert can occur as follows:

1) if the UA is connected and on-line to the MS, the alert message will be sent to the UA as soon as a message arrives at the MS that safisfies the registered criteria for generating alerts. If the UA is off line then the next time the UA connects to his MS after a message arrives at the MS satisfying the registered criteria, the user will be informed that one or more alert cases have occurred, the details of which can be determined by performing a Stored Message Summary;
2) in addition to, or as an alternative to 1) above, the MS can use other mechanisms to inform the user.

B.83 *Stored message auto-forward* MS

This element of service allows a user of an MS to register requests that the MS auto-forward selected messages that are delivered to it. The user of the MS can select through registration several sets of criteria chosen from the attributes available in the MS, and messages meeting each set of criteria will be auto-forwarded to one or more users or DLs. One text per selection criteria can also be specified to be included with each auto-forwarded message.

B.84 *Stored message deletion* MS

This element of service enables a recipient UA to delete certain of its messages from the MS. Messages cannot be deleted if they have not been previously listed.

B.85 *Stored message fetching* MS

This element of service enables a recipient UA to fetch from the MS a message, or portions of a message. The UA can fetch a message (or message portion) based on the same search criteria that can be used for stored message listing.

B.86 *Stored message listing* MS

This element of service provides a recipient UA with a list of information about certain of its messages stored in the MS. The information comprises selected attributes from a message's envelope and content and others added by the MS. The UA can limit the number of messages that will be listed.

B.87 *Stored message summary* MS

This element of service provides a recipient UA with a count of the number of messages satisfying a specified criteria based on one or more attributes of the message stored in the MS.

B.88 *Subject indication* IPM

This element of service allows the originator to indicate to the recipient(s) the subject of an IP-message being sent. The subject information is to be made available to the recipient.

B.89 *Submission time stamp indication* MT

This element of service enables the MTS to indicate to the originating UA and each recipient UA the date and time at which a message was submitted to the MTS. In the case of physical delivery, this element of service also enables the PDAU to indicate the date and time of submission on the physical message.

B.90 *Typed body* IPM

This element of service permits the nature and attributes of the body of the IP-message to be conveyed along with the body. Because the body can undergo conversion, the body type can change over time.

B.91 *Undeliverable mail with return of physical message* PD PR

This element of service enables the PDS to return the physical message without delay, with reason indicated to the originator, if it cannot be delivered to the addressee. This is the default action to be taken by the PDS.

*Note* – In the case of "poste restante" the return of the physical message will take place after some period of time.

B.92 *Use of distribution list* MT PR

This element of service enables an originating UA to specify a distribution list in place of all the individual recipients (users or nested LDs) mentioned therein. The MTS will add the members of the list to the recipients of the message and send it to those members. Distribution lists can be members of distribution lists, in which case the list of recipients can be successively expanded at several places in the MTS.

B.93 *User/UA capabilities registration* MT

This element of service enables a UA to indicate to its MTA, through registration, the unrestricted use of any or all of the following capabilities with respect to received messages:

1) the content type(s) of messages it is willing to have delivered to it;

2) the maximum content length of a message it is willing to have delivered to it;

3) the encoded information type(s) of messages it is willing to have delivered to it.

The MTA will not deliver to a UA a message that does not match, or exceeds, the capabilities registered.

ANNEX C

(to Recommendation F.400)

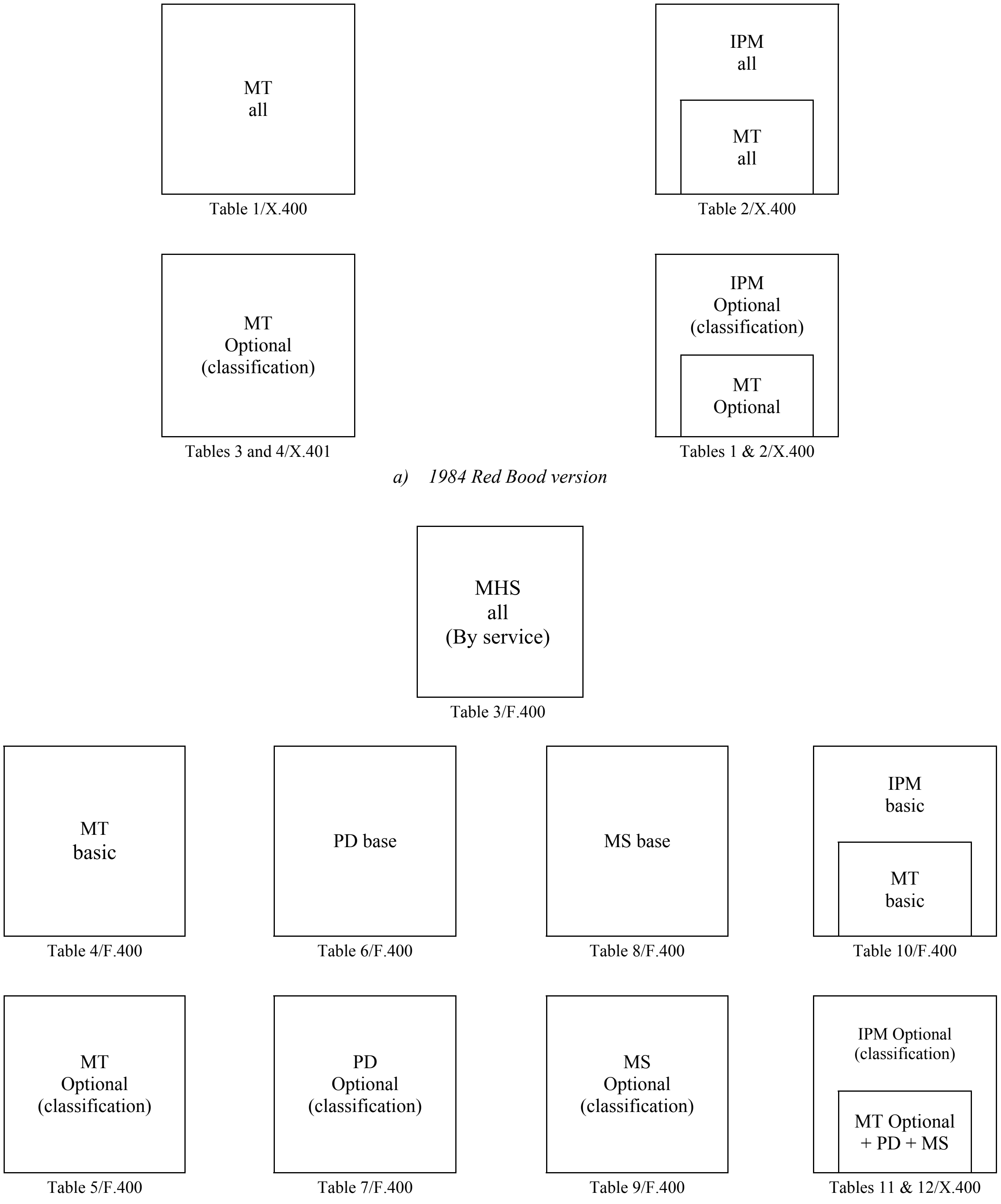
## Elements of service modifications with respect to the 1984 version

C.1 *New elements of service in 1988* (see Table C-1/F.400)

TABLE C-1/F.400

| Elements of service | MT | IPM | PD | MS | Annex B ref. |
|---|---|---|---|---|---|
| Additional physical rendition | | | X | | B.2 |
| Basic physical rendition | | | X | | B.7 |
| Content confidentiality | X | | | | B.10 |
| Content integrity | X | | | | B.11 |
| Conversion prohibition in case of loss of information | X | | | | B.14 |
| Counter collection | | | X | | B.16 |
| Counter collection with advice | | | X | | B.17 |
| Delivery via bureaufax service | | | X | | B.23 |
| Designation of recipient by directory name | X | | | | B.24 |
| DL expansion history indication | X | | | | B.26 |
| DL expansion prohibited | X | | | | B.27 |
| EMS (express mail service) | | | X | | B.28 |
| Incomplete copy indication | | X | | | B.36 |
| Language indication | | X | | | B.38 |
| Latest delivery designation | X | | | | B.39 |
| Message flow confidentiality | X | | | | B.40 |
| Message origin authentication | X | | | | B.42 |
| Message security labelling | X | | | | B.43 |
| Message sequence integrity | X | | | | B.44 |
| Non-repudiation of delivery | X | | | | B.49 |
| Non-repudiation of origin | X | | | | B.50 |
| Non-repudiation of submission | X | | | | B.51 |
| Ordinary mail | | | X | | B.53 |
| 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 forwarding prohibited | | | X | | B.60 |
| Probe origin authentication | X | | | | B.64 |
| Proof of delivery | X | | | | B.65 |
| Proof of submission | X | | | | B.66 |
| Redirection d is allowed by originator | X | | | | B.68 |
| Redirection of incoming messages | X | | | | B.69 |
| Registered mail | | | X | | B.70 |
| Reigstered mail to addressee in person | | | X | | B.71 |
| Report origin authentication | X | | | | B.74 |
| Request for forwarding address | | | X | | B.75 |
| Request delivery method | X | | | | B.76 |
| Request delivery | X | | | | B.77 |
| Secure access management | X | | | | B.79 |
| 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 |
| Undeliverable mail with return of physical message | | | X | | B.91 |
| Use of distribution list | X | | | | B.92 |
| User/UA capabilities registration | X | | | | B.93 |

### C.2 *Mapping of the 1984 and 1988 elements of service tables (see Figure C-1/F.400)*



*a) 1984 Red Bood version*

*b) 1988 Blue book version (F.400)*

FIGURE C-1/F.400

**Mapping of elements of service tables**

### C.3 *Classification of new elements of service*

The new elements of service that were added to the 1984 X.400-Series to create the 1988 F.400/X.400-Series Recommendations are all classified as additional optional user facilities with the following exceptions:

#### C.3.1 *MT service*

- DL expansion history indication;
- requested delivery method.

#### C.3.2 *IPM service*

- DL expansion history indication;
- language indication;
- requested delivery method.

#### C.3.3 *MH/PD service intercommunication*

Although some of the elements of service used in this intercommunication are classified as *Base* (see F.400, § 19.4), and some are classified as essential optional user facilities (see F.400, § 19.5), the provision of MH/PD service intercommunication is an option itself. When this intercommunication is provided, the base elements of service and optional user facilities shall be supported as classified in this Recommendation.

#### C.3.4 *Message store*

Although some of the elements of service used with the message store are classified as *Base* (see F.400, § 19.6), and others are classified as essential optional user facilities (see F.400, § 19.7), the provision of a message store is itself an option, and therefore the classifications are applicable only for the provider of a message store.

### C.4 *Changes in classification of 1984 elements of service*

All the elements of service in 1984 have retained their 1984 classifications with the following exception:

- Non-receipt notification request.

#### C.4.1 *Miscellaneous changes*

The element of service registered encoded information types in 1984 is now called user/UA capabilities registration and it has been extended in functionality.

Some of the 1984 element of service definitions have been revised editorially for ease of reading.

## ANNEX D

(to Recommendation F.400)

## **Differences between CCITT Recommendation F.400 and ISO Standard 10021-1**

(This Annex is not a part of this Recommendation)

This Annex points out the major differences between this Recommendation and the corresponding ISO International Standard. Because the differences in many cases involve the inclusion or exclusion of a word, a phrase, or a sentence, and these occur in many places throughout the text, this Annex does not specifically point to these instances. Rather it summarizes the intent of these differences.

The following are the major differences:

1) The CCITT text makes references throughout to CCITT services and their relationship to MHS;
2) Figure 5/F.400 showing relationships between management domains and corresponding notes;
3) Roles of ADMD and PRMD in naming;
4) Use of MHS in provision of public services (§ 17);
5) The Note about responsibility for storing deferred delivery messages (Annex B, § B.19) is not included in the ISO text.

## ITU-T F-SERIES RECOMMENDATIONS

## NON-TELEPHONE TELECOMMUNICATION SERVICES

| | |
|---|---|
| TELEGRAPH SERVICE | |
| Operating methods for the international public telegram service | F.1–F.19 |
| The gentex network | F.20–F.29 |
| Message switching | F.30–F.39 |
| The international telemessage service | F.40–F.58 |
| The international telex service | F.59–F.89 |
| Statistics and publications on international telegraph services | F.90–F.99 |
| Scheduled and leased communication services | F.100–F.104 |
| Phototelegraph service | F.105–F.109 |
| MOBILE SERVICE | |
| Mobile services and multidestination satellite services | F.110–F.159 |
| TELEMATIC SERVICES | |
| Public facsimile service | F.160–F.199 |
| Teletex service | F.200–F.299 |
| Videotex service | F.300–F.349 |
| General provisions for telematic services | F.350–F.399 |
| **MESSAGE HANDLING SERVICES** | **F.400–F.499** |
| DIRECTORY SERVICES | F.500–F.549 |
| DOCUMENT COMMUNICATION | |
| Document communication | F.550–F.579 |
| Programming communication interfaces | F.580–F.599 |
| DATA TRANSMISSION SERVICES | F.600–F.699 |
| AUDIOVISUAL SERVICES | F.700–F.799 |
| ISDN SERVICES | F.800–F.849 |
| UNIVERSAL PERSONAL TELECOMMUNICATION | F.850–F.899 |
| HUMAN FACTORS | F.900–F.999 |

*For further details, please refer to ITU-T List of Recommendations.*

ITU-T X-SERIES RECOMMENDATIONS

**DATA NETWORKS AND OPEN SYSTEM COMMUNICATIONS**

| | |
|---|---|
| PUBLIC DATA NETWORKS | |
| Services and facilities | X.1–X.19 |
| Interfaces | X.20–X.49 |
| Transmission, signalling and switching | X.50–X.89 |
| Network aspects | X.90–X.149 |
| Maintenance | X.150–X.179 |
| Administrative arrangements | X.180–X.199 |
| OPEN SYSTEMS INTERCONNECTION | |
| Model and notation | X.200–X.209 |
| Service definitions | X.210–X.219 |
| Connection-mode protocol specifications | X.220–X.229 |
| Connectionless-mode protocol specifications | X.230–X.239 |
| PICS proformas | X.240–X.259 |
| Protocol Identification | X.260–X.269 |
| Security Protocols | X.270–X.279 |
| Layer Managed Objects | X.280–X.289 |
| Conformance testing | X.290–X.299 |
| INTERWORKING BETWEEN NETWORKS | |
| General | X.300–X.349 |
| Satellite data transmission systems | X.350–X.399 |
| **MESSAGE HANDLING SYSTEMS** | **X.400–X.499** |
| DIRECTORY | X.500–X.599 |
| OSI NETWORKING AND SYSTEM ASPECTS | |
| Networking | X.600–X.629 |
| Efficiency | X.630–X.639 |
| Quality of service | X.640–X.649 |
| Naming, Addressing and Registration | X.650–X.679 |
| Abstract Syntax Notation One (ASN.1) | X.680–X.699 |
| OSI MANAGEMENT | |
| Systems Management framework and architecture | X.700–X.709 |
| Management Communication Service and Protocol | X.710–X.719 |
| Structure of Management Information | X.720–X.729 |
| Management functions and ODMA functions | X.730–X.799 |
| SECURITY | X.800–X.849 |
| OSI APPLICATIONS | |
| Commitment, Concurrency and Recovery | X.850–X.859 |
| Transaction processing | X.860–X.879 |
| Remote operations | X.880–X.899 |

*For further details, please refer to ITU-T List of Recommendations.*

## ITU-T RECOMMENDATIONS SERIES

| | |
|---|---|
| Series A | Organization of the work of the ITU-T |
| Series B | Means of expression: definitions, symbols, classification |
| Series C | General telecommunication statistics |
| Series D | General tariff principles |
| Series E | Overall network operation, telephone service, service operation and human factors |
| **Series F** | **Non-telephone telecommunication services** |
| Series G | Transmission systems and media, digital systems and networks |
| Series H | Audiovisual and multimedia systems |
| Series I | Integrated services digital network |
| Series J | Transmission of television, sound programme and other multimedia signals |
| Series K | Protection against interference |
| Series L | Construction, installation and protection of cables and other elements of outside plant |
| Series M | TMN and network maintenance: international transmission systems, telephone circuits, telegraphy, facsimile and leased circuits |
| Series N | Maintenance: international sound programme and television transmission circuits |
| Series O | Specifications of measuring equipment |
| Series P | Telephone transmission quality, telephone installations, local line networks |
| Series Q | Switching and signalling |
| Series R | Telegraph transmission |
| Series S | Telegraph services terminal equipment |
| Series T | Terminals for telematic services |
| Series U | Telegraph switching |
| Series V | Data communication over the telephone network |
| **Series X** | **Data networks and open system communications** |
| Series Y | Global information infrastructure and Internet protocol aspects |
| Series Z | Languages and general software aspects for telecommunication systems |

Printed in Switzerland
Geneva, 2007