INTERNATIONAL TELECOMMUNICATION UNION

CCITT

THE INTERNATIONAL
TELEGRAPH AND TELEPHONE
CONSULTATIVE COMMITTEE

BLUE BOOK

VOLUME II – FASCICLE II.6

MESSAGE HANDLING AND DIRECTORY SERVICES OPERATIONS AND DEFINITION OF SERVICE

RECOMMENDATIONS F.400-F.422, F.500

IXTH PLENARY ASSEMBLY
MELBOURNE, 14-25 NOVEMBER 1988

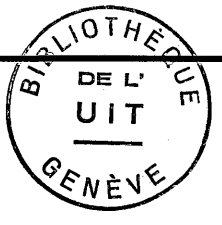
Geneva 1989

INTERNATIONAL TELECOMMUNICATION UNION

CCITT

THE INTERNATIONAL
TELEGRAPH AND TELEPHONE
CONSULTATIVE COMMITTEE

BLUE BOOK



VOLUME II – FASCICLE II.6

MESSAGE HANDLING AND DIRECTORY SERVICES OPERATIONS AND DEFINITION OF SERVICE

RECOMMENDATIONS F.400-F.422, F.500

IXTH PLENARY ASSEMBLY
MELBOURNE, 14-25 NOVEMBER 1988

Geneva 1989

ISBN 92-61-03301-6

Printed in Switzerland

CONTENTS OF THE CCITT BOOK
APPLICABLE AFTER THE NINTH PLENARY ASSEMBLY (1988)

BLUE BOOK

FASCICLE III.6 – Line transmission of non-telephone signals. Transmission of sound-programme and television signals. Series H and J Recommendations (Study Group XV).

FASCICLE III.7 – Integrated Services Digital Network (ISDN) – General structure and service capabilities. Recommendations I.110-I.257 (Study Group XVIII).

FASCICLE III.8 – Integrated Services Digital Network (ISDN) – Overall network aspects and functions, ISDN user-network interfaces. Recommendations I.310-I.470 (Study Group XVIII).

FASCICLE III.9 – Integrated Services Digital Network (ISDN) – Internetwork interfaces and maintenance principles. Recommendations I.500-I.605 (Study Group XVIII).

Volume IV

FASCICLE IV.1 – General maintenance principles: maintenance of international transmission systems and telephone circuits. Recommendations M.10-M.782 (Study Group IV).

FASCICLE IV.2 – Maintenance of international telegraph, phototelegraph and leased circuits. Maintenance of the international public telephone network. Maintenance of maritime satellite and data transmission systems. Recommendations M.800-M.1375 (Study Group IV).

FASCICLE IV.3 – Maintenance of international sound-programme and television transmission circuits. Series N Recommendations (Study Group IV).

FASCICLE IV.4 – Specifications for measuring equipment. Series O Recommendations (Study Group IV).

Volume V – Telephone transmission quality. Series P Recommendations (Study Group XII).

Volume VI

FASCICLE VI.1 – General Recommendations on telephone switching and signalling. Functions and information flows for services in the ISDN. Supplements. Recommendations Q.1-Q.118 *bis* (Study Group XI).

FASCICLE VI.2 – Specifications of Signalling Systems Nos. 4 and 5. Recommendations Q.120-Q.180 (Study Group XI).

FASCICLE VI.3 – Specifications of Signalling System No. 6. Recommendations Q.251-Q.300 (Study Group XI).

FASCICLE VI.4 – Specifications of Signalling Systems R1 and R2. Recommendations Q.310-Q.490 (Study Group XI).

FASCICLE VI.5 – Digital local, transit, combined and international exchanges in integrated digital networks and mixed analogue-digital networks. Supplements. Recommendations Q.500-Q.554 (Study Group XI).

FASCICLE VI.6 – Interworking of signalling systems. Recommendations Q.601-Q.699 (Study Group XI).

FASCICLE VI.7 – Specifications of Signalling System No. 7. Recommendations Q.700-Q.716 (Study Group XI).

FASCICLE VI.8 – Specifications of Signalling System No. 7. Recommendations Q.721-Q.766 (Study Group XI).

FASCICLE VI.9 – Specifications of Signalling System No. 7. Recommendations Q.771-Q.795 (Study Group XI).

FASCICLE VI.10 – Digital subscriber signalling system No. 1 (DSS 1), data link layer. Recommendations Q.920-Q.921 (Study Group XI).

FASCICLE VI.11 – Digital subscriber signalling system No. 1 (DSS 1), network layer, user-network management. Recommendations Q.930-Q.940 (Study Group XI).

FASCICLE VI.12 – Public land mobile network. Interworking with ISDN and PSTN. Recommendations Q.1000-Q.1032 (Study Group XI).

FASCICLE VI.13 – Public land mobile network. Mobile application part and interfaces. Recommendations Q.1051-Q.1063 (Study Group XI).

FASCICLE VI.14 – Interworking with satellite mobile systems. Recommendations Q.1100-Q.1152 (Study Group XI).

Volume VII

FASCICLE VII.1 – Telegraph transmission. Series R Recommendations. Telegraph services terminal equipment. Series S Recommendations (Study Group IX).

FASCICLE VII.2 – Telegraph switching. Series U Recommendations (Study Group IX).

FASCICLE VII.3 – Terminal equipment and protocols for telematic services. Recommendations T.0-T.63 (Study Group VIII).

FASCICLE VII.4 – Conformance testing procedures for the Teletex Recommendations. Recommendation T.64 (Study Group VIII).

FASCICLE VII.5 – Terminal equipment and protocols for telematic services. Recommendations T.65-T.101, T.150-T.390 (Study Group VIII).

FASCICLE VII.6 – Terminal equipment and protocols for telematic services. Recommendations T.400-T.418 (Study Group VIII).

FASCICLE VII.7 – Terminal equipment and protocols for telematic services. Recommendations T.431-T.564 (Study Group VIII).

Volume VIII

FASCICLE VIII.1 – Data communication over the telephone network. Series V Recommendations (Study Group XVII).

FASCICLE VIII.2 – Data communication networks: services and facilities, interfaces. Recommendations X.1-X.32 (Study Group VII).

FASCICLE VIII.3 – Data communication networks: transmission, signalling and switching, network aspects, maintenance and administrative arrangements. Recommendations X.40-X.181 (Study Group VII).

FASCICLE VIII.4 – Data communication networks: Open Systems Interconnection (OSI) – Model and notation, service definition. Recommendations X.200-X.219 (Study Group VII).

FASCICLE VIII.5 – Data communication networks: Open Systems Interconnection (OSI) – Protocol specifications, conformance testing. Recommendations X.220-X.290 (Study Group VII).

FASCICLE VIII.6 – Data communication networks: interworking between networks, mobile data transmission systems, internetwork management. Recommendations X.300-X.370 (Study Group VII).

FASCICLE VIII.7 – Data communication networks: message handling systems. Recommendations X.400-X.420 (Study Group VII).

FASCICLE VIII.8 – Data communication networks: directory. Recommendations X.500-X.521 (Study Group VII).

Volume IX – Protection against interference. Series K Recommendations (Study Group V). Construction, installation and protection of cable and other elements of outside plant. Series L Recommendations (Study Group VI).

Volume X

FASCICLE X.1 – Functional Specification and Description Language (SDL). Criteria for using Formal Description Techniques (FDTs). Recommendation Z.100 and Annexes A, B, C and E, Recommendation Z.110 (Study Group X).

FASCICLE X.2 – Annex D to Recommendation Z.100: SDL user guidelines (Study Group X).

FASCICLE X.3 – Annex F.1 to Recommendation Z.100: SDL formal definition. Introduction (Study Group X).

FASCICLE X.4 – Annex F.2 to Recommendation Z.100: SDL formal definition. Static semantics (Study Group X).

FASCICLE X.5 – Annex F.3 to Recommendation Z.100: SDL formal definition. Dynamic semantics (Study Group X).

FASCICLE X.6 – CCITT High Level Language (CHILL). Recommendation Z.200 (Study Group X).

FASCICLE X.7 – Man-Machine Language (MML). Recommendations Z.301-Z.341 (Study Group X).

CONTENTS OF FASCICLE II.6 OF THE BLUE BOOK

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

Message handling and directory services – Operations and definition of service

MODIFICATIONS TO THE F-SERIES RECOMMENDATIONS

1 *Fascicle II.4*

1.1 The following new Recommendations and Supplements did not appear in Fascicle II.4 of the Red Book and were developed during the 1985-1988 Study Period;

Recommendations

F.4
F.50
F.51
F.73
F.74
F.75 (the same as F.421, the text is found in Fascicle II.6)
F.125
F.126
F.127
F.140

Supplements

No. 2
No. 3

1.2 The following Recommendations and Supplements in Fascicle II.4 of the Red Book were revised during the 1985-1988 Study Period:

Recommendations

F.1
F.30
F.31
F.41
F.42
F.60
F.61
F.70
F.71
F.72
F.80
F.80 *bis*
F.85
F.110
F.120
F.122

Supplement

No. 1

1.3 The following Recommendations have been transferred to the D-series Recommendations and no longer appear in Fascicle II.4 of the Blue Book:

Recommendations

F.43
F.45
F.66
F.67
F.83
F.111

1.4 The following Recommendations have been deleted from the F-series and no longer appear in the Blue Book:

Recommendations

F.2 [1)]
F.79 [1)]
F.121

1.5 The number of Recommendation F.150 has been changed to F.35, and now appears in Section 3 of Fascicle II.4.

---

1) See instead Recommendation C.3 *Instructions for international telecommunication services*, Volume I, *Blue Book*.

2 *Fascicle II.5*

2.1 The following new Recommendations did not appear in Fascicle II.5 of the Red Book and were developed during the 1985-1988 Study Period:

Recommendations

F.171
F.202
F.203
F.220
F.230
F.351
F.353
F.600
F.601
F.710
F.721
F.730

2.2 The following Recommendations in Fascicle II.5 of the Red Book were revised during the 1985-1988 Study Period:

Recommendations

F.160
F.162
F.170
F.180
F.182 (new number, formerly § 5 of Rec. F.180)
F.184 (new number, formerly F.161)
F.190
F.200
F.201
F.300

3 *New Fascicle II.6*

Fascicle II.6 is a new fascicle in the F-series and contains the following new Recommendations developed during the 1985-1988 Study Period:

Recommendations

F.400
F.401
F.410
F.415
F.420
F.421 (F.75)
F.422
F.500

PRELIMINARY NOTES

1 The Questions entrusted to each Study Group for the Study Period 1989-1992 can be found in Contribution No. 1 to that Study Group.

2 In this Fascicle, the expression "Administration" is used for shortness to indicate both a telecommunication Administration and a recognized private operating agency.

FASCICLE II.6

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

MESSAGE HANDLING AND DIRECTORY SERVICES – OPERATIONS AND DEFINITION OF SERVICE

PAGE INTENTIONALLY LEFT BLANK

PAGE LAISSEE EN BLANC INTENTIONNELLEMENT

PROTECTION OF THE COMMON NAMES OF CCITT DEFINED INTERNATIONAL PUBLIC SERVICES

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

Resolution No. 13

PROTECTION OF THE COMMON NAMES OF CCITT DEFINED INTERNATIONAL PUBLIC SERVICES

(Geneva, 1980)

The CCITT,

considering

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

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

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

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

noting

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

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

resolves to request Administrations

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

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

(3) to ensure that in the case of a combination of any such CCITT defined international public services together with further optional user facilities in addition to that basic service, the trade mark or the service mark for such a combined service offered by any RPOA be always combined with the respective common name of the basic CCITT defined international public service, i.e. "teletex", "telefax" or "bureaufax", and that the latter names, in the case of registration of such a trade mark or service mark, be made the subject of a disclaimer;

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

requests the Director of the CCITT

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

SECTION 1

MESSAGE HANDLING SERVICES

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.

---

[1] Recommendation X.400 is identical to F.400.

CONTENTS

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	9072-2		

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 10021-3)

Recommendation X.408 Message handling systems – Encoded information type convention rules

Recommendation X.411 Message handling systems – Message transfer system: Abstract service definition and procedures (see also ISO/IEC 10021-4)

Recommendation X.413 Message handling systems – Message store: Abstract service definition (see also ISO/IEC 10021-5)

Recommendation X.419 Message handling systems – Protocol specifications (see also ISO/IEC 10021-6)

Recommendation X.420 Message handling systems – Interpersonal messaging system (see also ISO/IEC 10021-7)

Recommendation X.500 Directory – Overview (see also ISO/IEC 9594-1)

Recommendation X.501 Directory – Models (see also ISO/IEC 9594-2)

Recommendation X.509 Directory – Authentication (see also ISO/IEC 9594-8)

Recommendation X.511 Directory – Abstract service definition (see also ISO/IEC 9594-3)

Recommendation X.518 Directory – Procedures for distributed operations (see also ISO/IEC 9594-4)

Recommendation X.519 Directory – Protocol specifications (see also ISO/IEC 9594-5)

Recommendation X.520 Directory – Selected attribute types (see also ISO/IEC 9594-6)

Recommendation X.521 Directory – Selected object classes (see also ISO/IEC 9594-7)

3 Definitions

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

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

3.1 *Open systems interconnection*

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

a) Application layer;
b) Application-process;
c) Open systems interconnection;
d) OSI reference model.

3.2 *Directory systems*

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

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

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

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

4 Abbreviations

A	Additional
ADMD	Administration management domain
AU	Access unit
CA	Contractual agreement
DL	Distribution list
DSA	Directory system agent
DUA	Directory user agent

E	Essential
EIT	Encoded information type
I/O	Input/output
IP	Interpersonal
IPM	Interpersonal messaging
IPMS	Interpersonal messaging system
MD	Management domain
MH	Message handling
MHS	Message handling system
MS	Message store
MT	Message transfer
MTA	Message transfer agent
MTS	Message transfer system
N/A	Not applicable
O/R	Originator/recipient
OSI	Open system interconnection
PD	Physical delivery
PDAU	Physical delivery access unit
PDS	Physical delivery system
PM	Per-message
PR	Per-recipient
PRMD	Private management domain
PTLXAU	Public telex access unit
TLMA	Telematic agent
TLXAU	Telex access unit
TTX	Teletex
UA	User agent

5 Conventions

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

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

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.

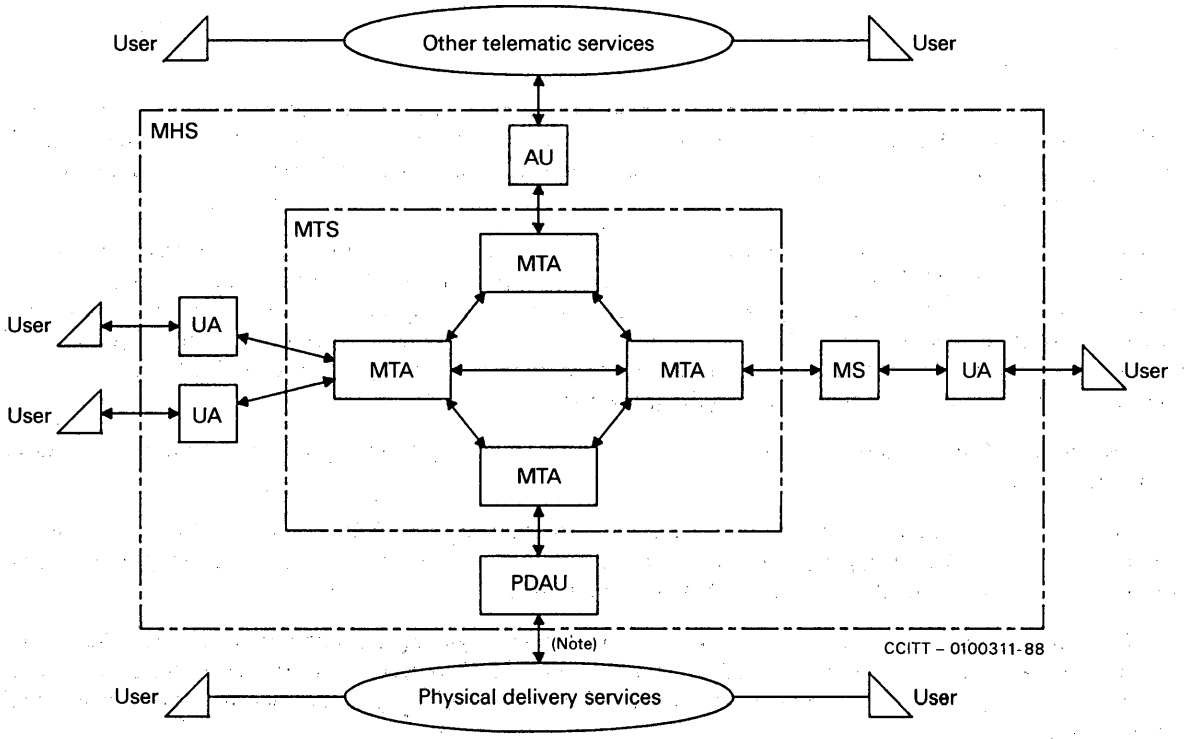
An originator prepares messages with the assistance of his user agent. A user agent (UA) is an application process that interacts with the message transfer system (MTS) or a message store (MS), to submit messages on behalf of a single user. The MTS delivers the messages submitted to it, to one or more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

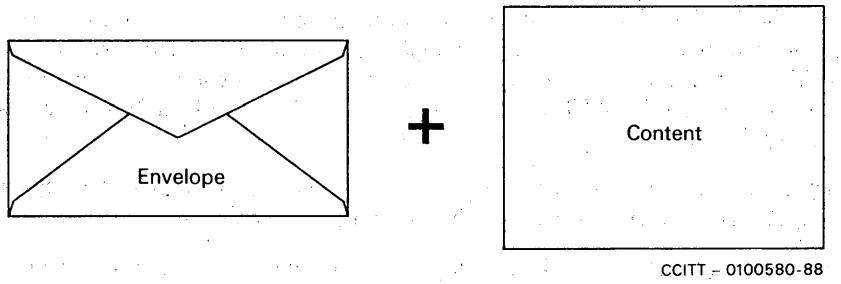


FIGURE 2/F.400

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.

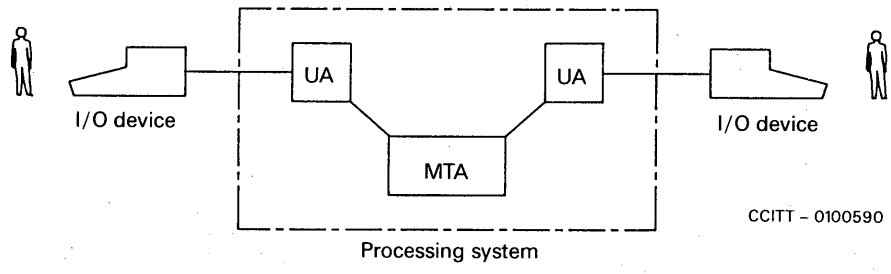


FIGURE 3/F.400

Co-resident UA and MTA

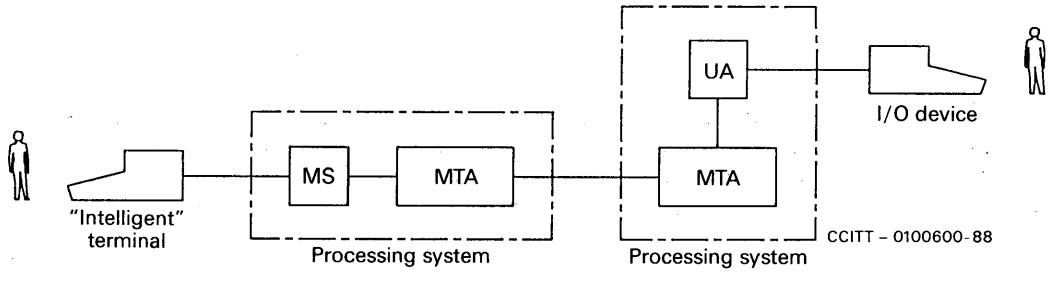


FIGURE 4/F.400

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.

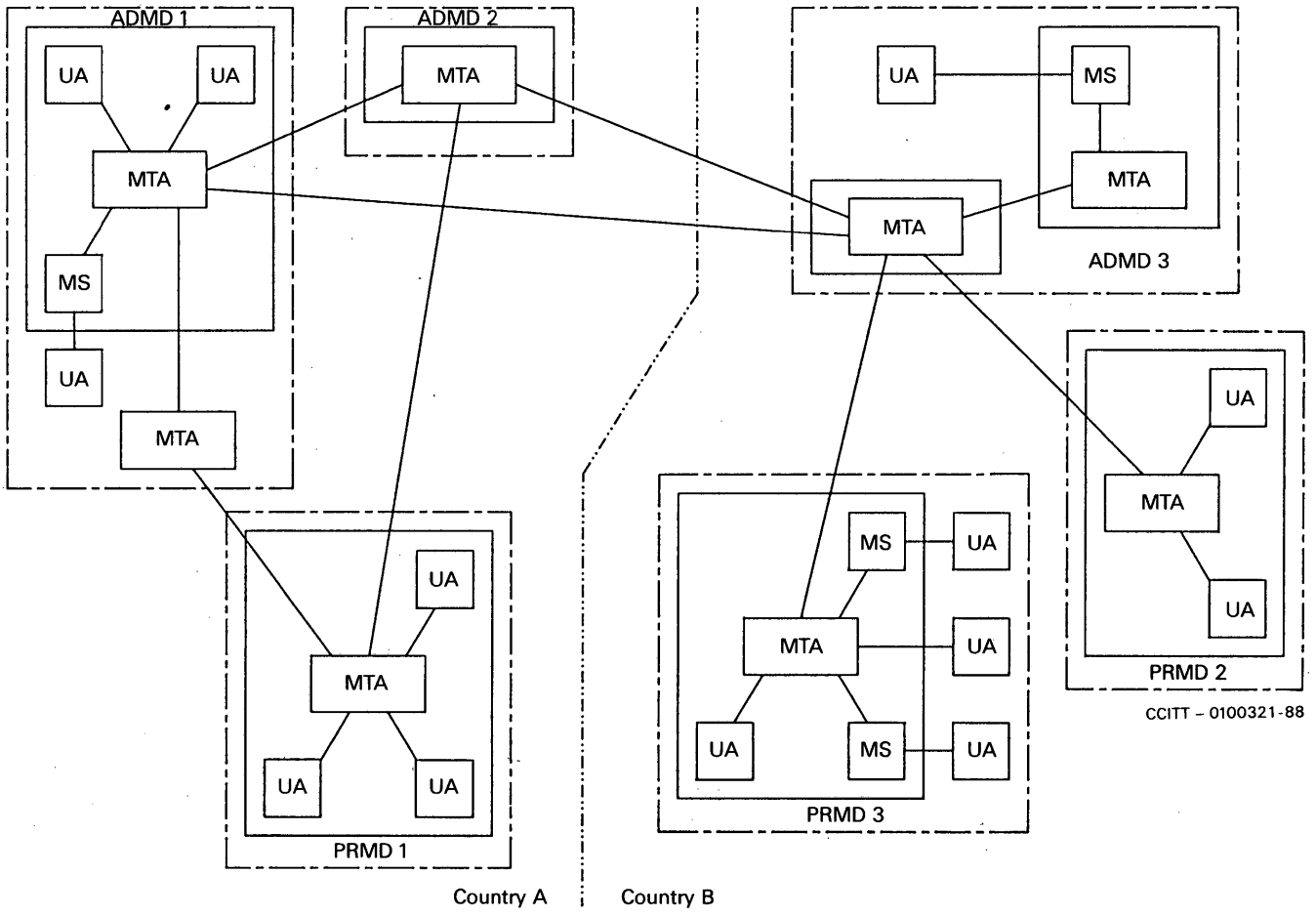


FIGURE 5/F.400

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.

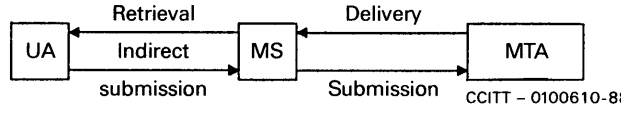


FIGURE 6/F.400

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.

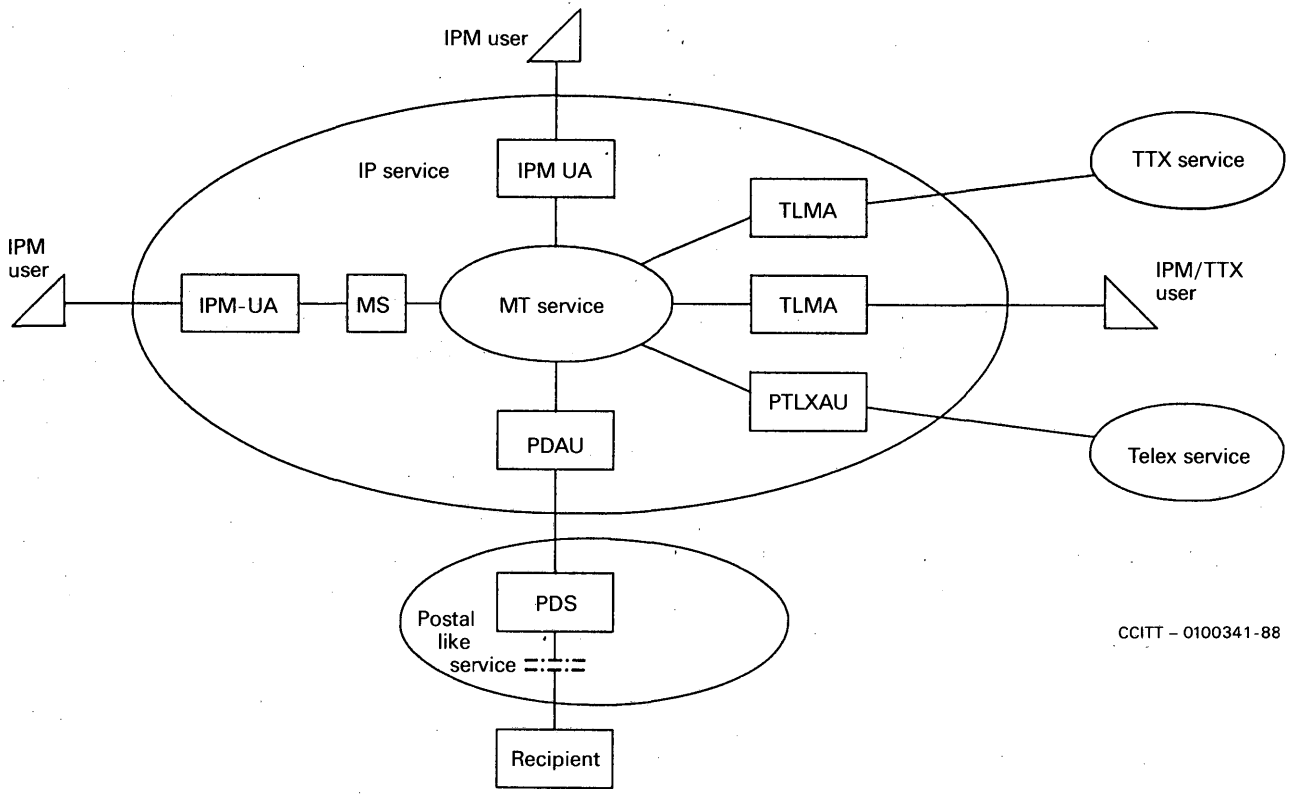


FIGURE 7/F.400

IPM service functional model

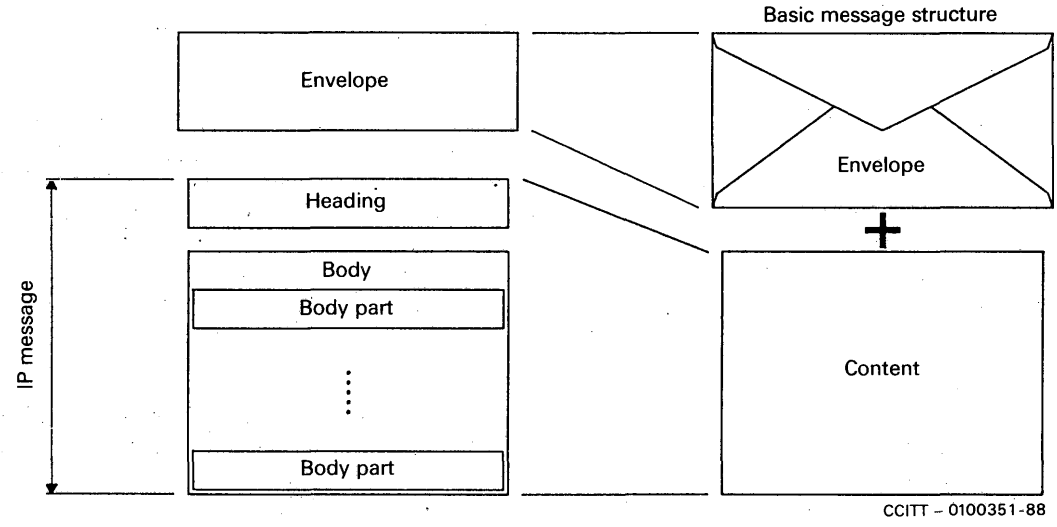


FIGURE 8/F.400

IP-message structure

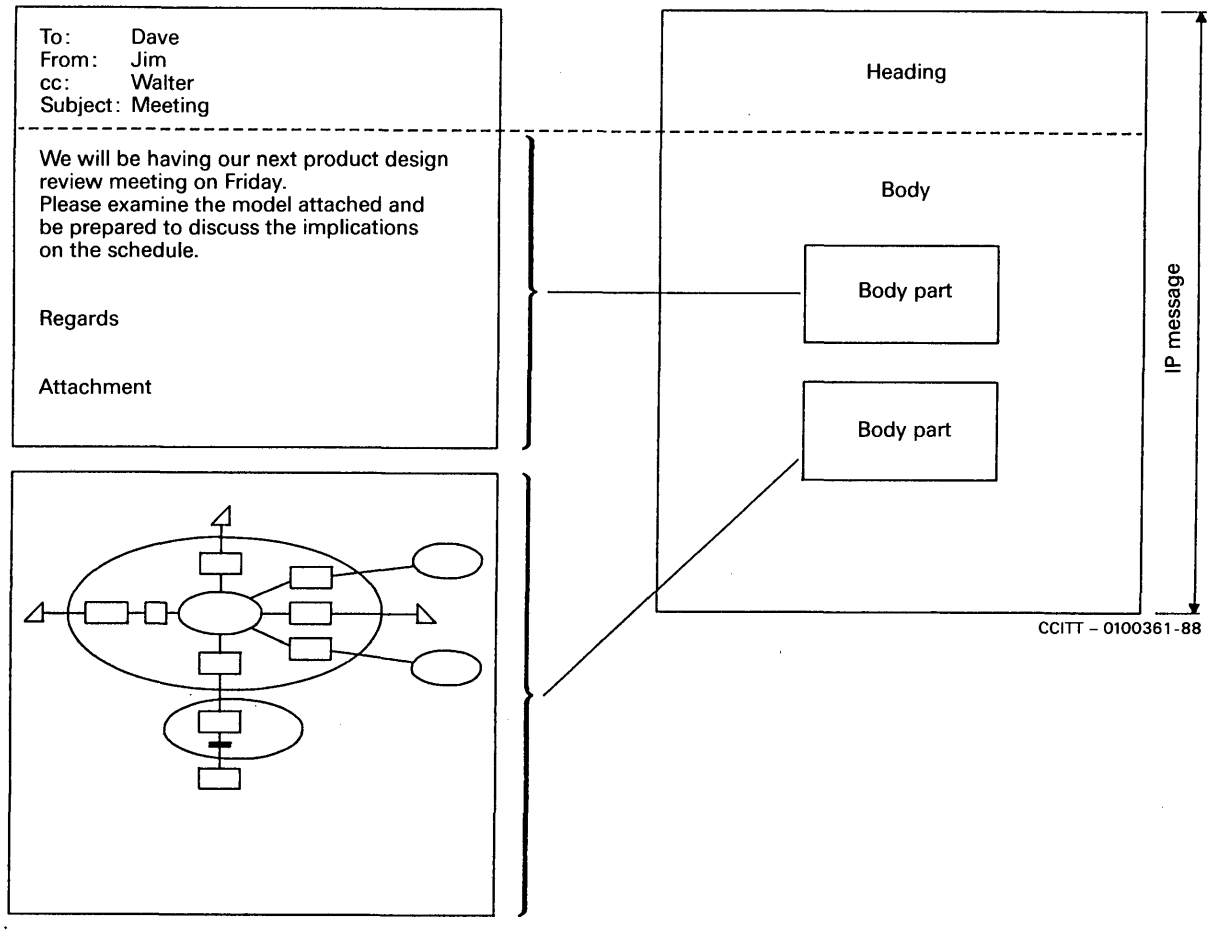


FIGURE 9/F.400

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.

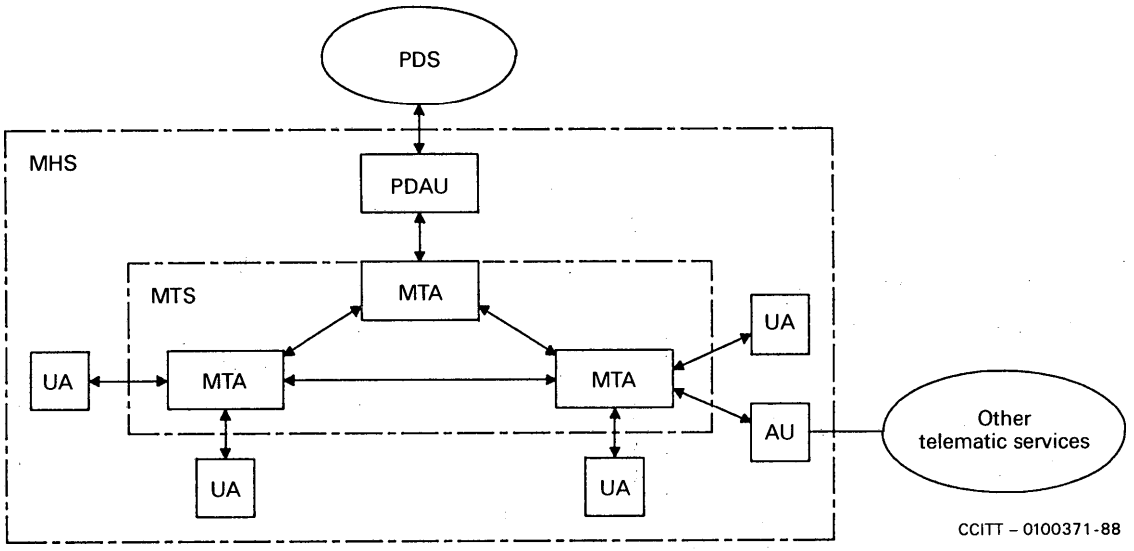


FIGURE 10/F.400

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.

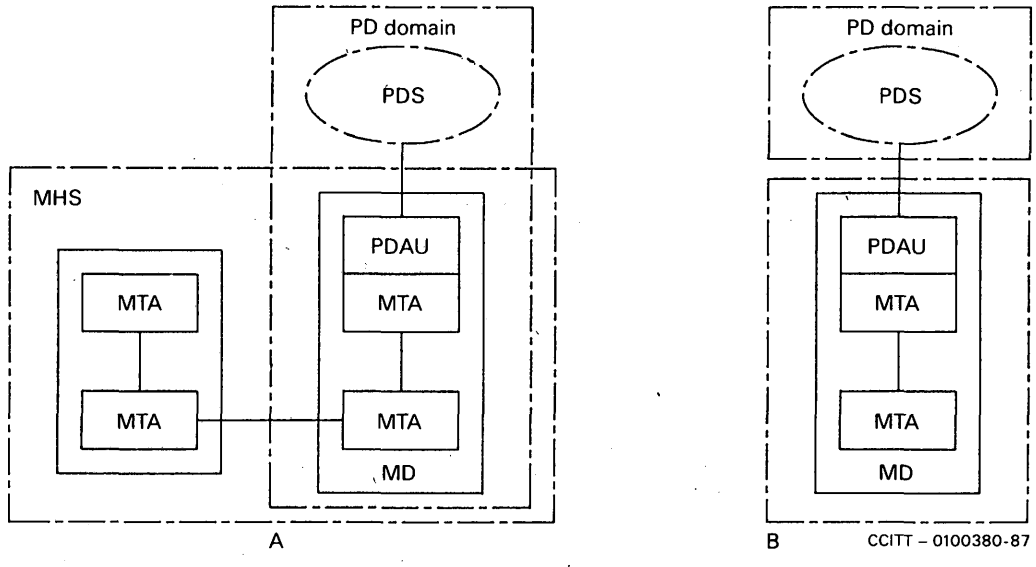


FIGURE 11/F.400

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.

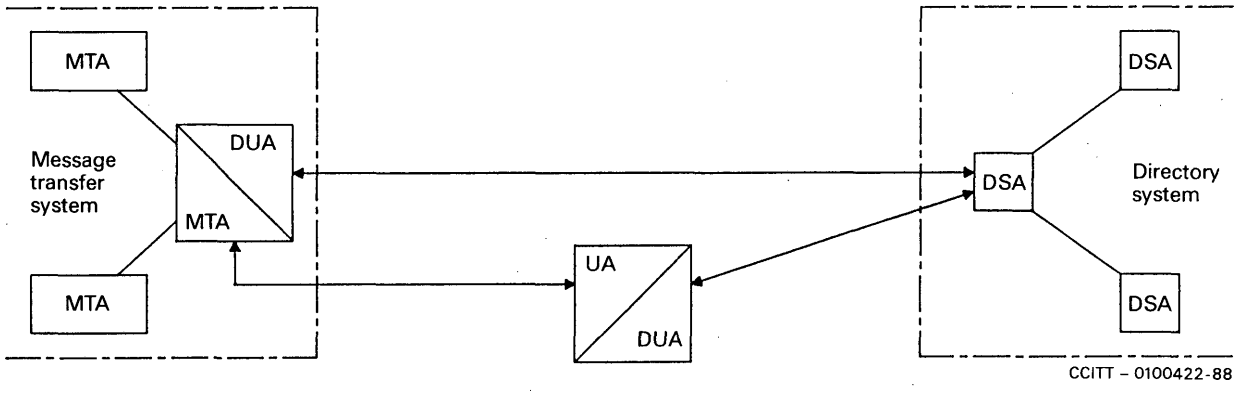


FIGURE 12/F.400

Functional model of 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.

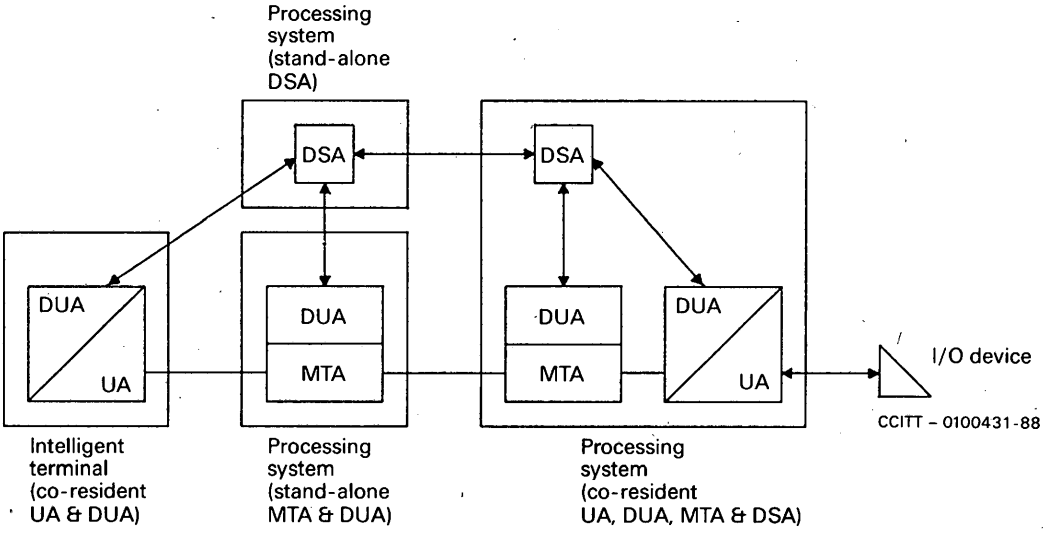


FIGURE 13/F.400

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.

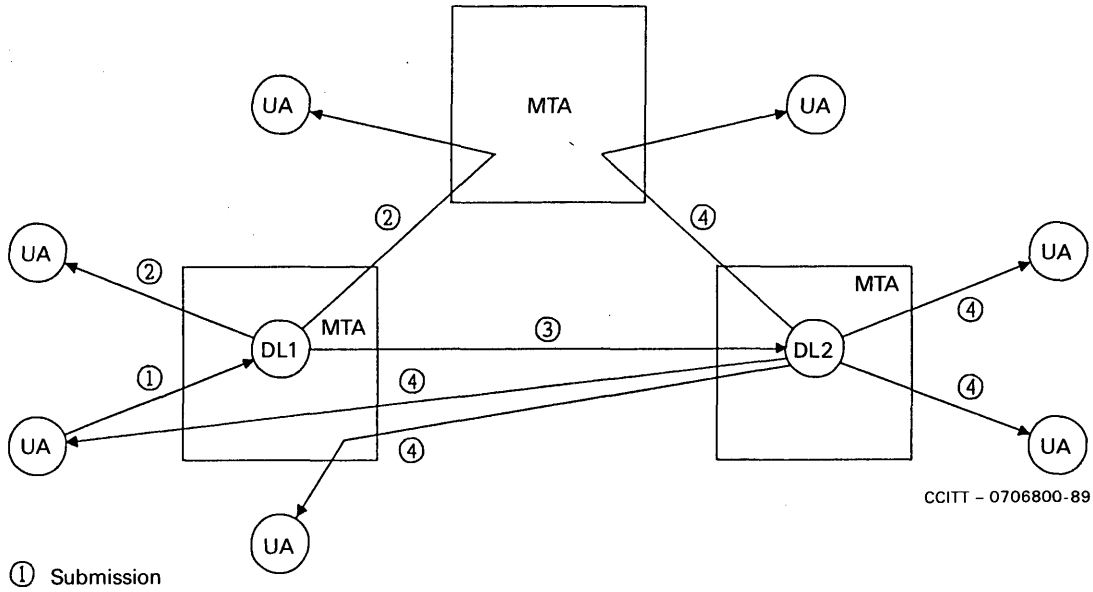


FIGURE 14/F.400

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.

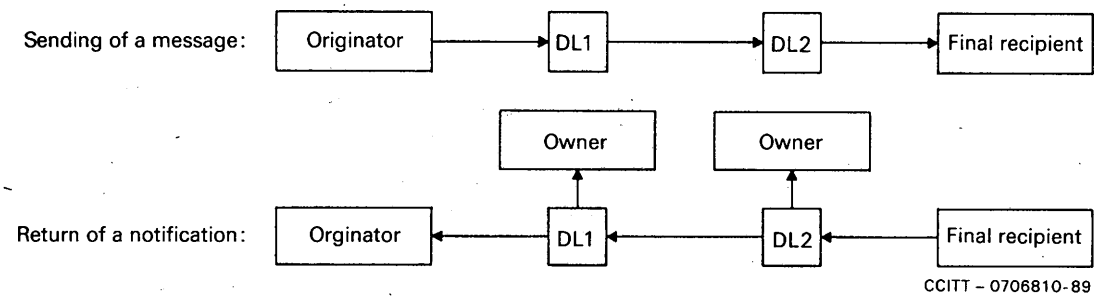


FIGURE 15/F.400

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.

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
Fowarded IP-message indication		X			B.31
Garde of delivery selection	X				B.32
Hold for delivery	X				B.33
Implicit conversion	X				B.34
Importance indication		X			B.35
Incomplete copy indication		X			B.36
IP-message identification		X			B.37
Language indication		X			B.38
Latest delivery designation	X				B.39
Message flow confidentiality	X				B.40
Message identification	X				B.41
Message origin authentication	X				B.42
Message security labelling	X				B.43
Message sequence integrity	X				B.44
Multi-destination delivery	X				B.45
Multi-part body		X			B.46
Non-delivery notification	X				B.47

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

Elements of service	MT	IPM	PD	MS	Annex B reference
Non-receipt notification request indication		X			B.48
Non-repudiation of delivery	X				B.49
Non-repudiation of origin	X				B.50
Non-repudiation of submission	X				B.51
Obsoleting indication		X			B.52
Ordinary mail			X		B.53
Original encoded information types indication	X				B.54
Originator indication		X			B.55
Originator requested alternate recipient	X				B.56
Physical delivery notification by MHS			X		B.57
Physical delivery notification by PDS			X		B.58
Physical forwarding allowed			X		B.59
Physical fowarding prohibited			X		B.60
Prevention of non-delivery notification	X				B.61
Primary and copy recipients indication		X			B.62
Probe	X				B.63
Probe origin authentication	X				B.64
Proof of delivery	X				B.65
Proof of submission	X				B.66
Receipt notification request indication		X			B.67
Redirection disallowed by originator	X				B.68
Redirection of incoming messages	X				B.69
Registered mail			X		B.70
Registered mail to addressee in person			X		B.71
Reply request indication		X			B.72
Replying IP-message indication		X			B.73
Report origin authentication	X				B.74
Request for forwarding address			X		B.75
Requested delivery method	X				B.76
Restricted delivery	X				B.77
Return of content	X				B.78
Secure access management	X				B.79
Sensitivity indication		X			B.80
Special delivery			X		B.81
Stored message alert				X	B.82
Stored message auto-forward				X	B.83
Stored message deletion				X	B.84
Stored message fetching				X	B.85
Stored message listing				X	B.86
Stored message summary				X	B.87
Subject indication		X			B.88
Submission time stamp indication	X				B.89
Type body		X			B.90
Undeliverable mail with return of physical message			X		B.91
Use of distribution list	X				B.92
User/UA capabilities registration	X				B.93

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
Deffered delivery	E	PM	B.19
Defered delivery cancellation	E	PM	B.20
Delivery notification	E	PM	B.21
Designation of recipient by directory name	A	PM	B.24
Disclosure of other recipients	E	PM	B.25
DL expansion history indication	E	PM	B.26
DL expansion prohibited	A	PM	B.27
Explicit conversion	A	PM	B.30
Grade of delivery selection	E	PM	B.32
Hold for delivery	A	CA	B.33
Implicit conversion	A	CA	B.34
Lastest delivery designation	A	PM	B.39
Message flow confidentiality	A	PM	B.40
Message origin authentication	A	PM	B.42
Message security labelling	A	PM	B.43
Message sequence integrity	A	PM	B.44
Multi-destination delivery	A	PM	B.45
Non-repudiation of delivery	A	PM	B.49
Non-repudiatation of origin	A	PM	B.50
Non-repudiation of submission	A	PM	B.51
Originator requested alternate recipient	A	PM	B.56
Prevention of non-delivery notification	A	PM	B.61
Probe	E	PM	B.63
Probe origin authentication	A	PM	B.64
Proof of delivery	A	PM	B.65
Proof of submission	A	PM	B.66
Redirection disallowed by originator	A	PM	B.68
Redirection of incoming messages	A	CA	B.69
Report origin authentication	A	PM	B.74
Requested delivery method	E [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 addressee 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

Elements of service belonging to the basic IPM service

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

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
Deffered delivery	E	N/A	B.19
Deffered delivery cancellation	A	N/A	B.20
Delivery notification	E	N/A	B.21
Delivery via Bureaufax service	A	A	B.23
Designation of recipient by directory name	A	N/A	B.24
Disclosure of other recipients	A	E	B.25
DL expansion history indication	N/A	E	B.26
DL expansion prohibited	A	A	B.27
EMS (express mail service) [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
Registred mail	A	A	B.70
Registred mail to addressee in person	A	A	B.71
Reply request indication	A	E	B.72
Reply IP-message indication	E	E	B.73
Report origin authentication	A	A	B.74
Request for forwarding address	A	A	B.75
Requested delivery method	E	N/A	B.76
Return of content	A	N/A	B.78
Sensitivity indication	A	E	B.80
Special delivery [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'accès (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 fisica (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 física (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 física

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 fisica (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* MT PR

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
Registered mail to addressee in person			X		B.71
Report origin authentication	X				B.74
Request for forwarding address			X		B.75
Requested delivery method	X				B.76
Restricted 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)

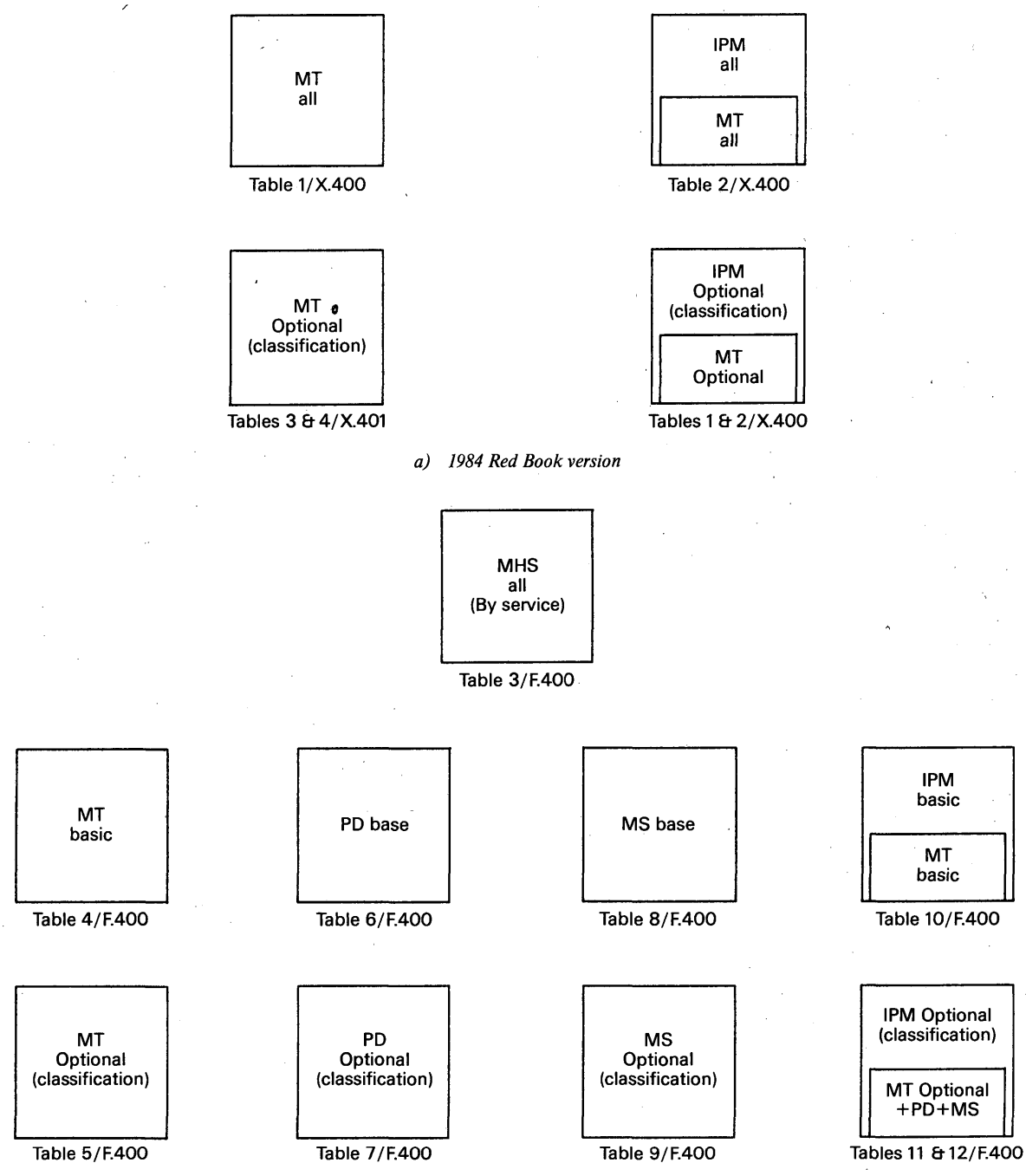


FIGURE C-1/F.400

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.

Recommendation F.401

MESSAGE HANDLING SERVICES: NAMING AND ADDRESSING FOR PUBLIC MESSAGE HANDLING SERVICES

The establishment in various countries of message handling services in association with public networks creates the need to produce Recommendations covering the aspects of public message handling services.

The CCITT,

considering

(a) The need for public message handling services;

(b) the strategic and commercial importance of standardization of message handling services;

(c) the urgent need for intercommunication arrangements for existing telematic services, and other services with public message handling services;

(d) the need for a clear distinction between the responsibilities to be allocated to service providers and those of subscribers and/or users;

(e) the need for establishing international compatibility between different messaging systems;

(f) the growth of the installed base of terminals and personal computers with the ability to access message handling systems;

(g) that several F series Recommendations describe public message handling services;

(h) that certain X and T series Recommendations cover relevant aspects of systems used for the provision of messaging services;

(i) that unambiguous names are required for the exchange of messages;

(j) that naming conventions are necessary for worldwide compatible services;

unanimously declares

the view that the naming and addressing requirements specified in this Recommendation should be applied for the provision of public message handling services.

CONTENTS

1 Purpose and scope

This Recommendation specifies naming and addressing aspects for public message handling services which are described in other Recommendations of the F-series. It also establishes some principles for the allocation of O/R addresses.

2 Naming and addressing in message handling

Naming and addressing in message handling have to ensure that users can define the source and the destination of messages in an unambiguous way. The organizational mapping of message handling systems, and the structure of management domains (see Recommendation F.400/X.400), together with a set of naming conventions, are the means to establish a uniform and compatible environment for the exchange of messages between any users of the message handling environment.

Names and addresses are allocated by the responsible naming authority.

In message handling systems (MHS), the principal entity that requires naming is the user (the originator and the recipient of messages). In addition distribution lists (DLs) have names for their use in the context of MHS. Users of MHs and DLs are identified by O/R names. (The prefix "O/R" recognizes the fact that the user can be acting as either the originator or the recipient of a message). An O/R name comprises a directory name, an O/R address or both. Every user or DL has one or more O/R names.

2.1 *O/R addresses*

An O/R address contains information that enables the MHS to identify a user to deliver a message or return a notification to him. DLs are also identified by an O/R address.

An O/R address is comprised of a set of information called attributes. Recommendation X.402 specifies a set of standard attributes from which O/R addresses can be constructed. Standard attributes, the structure of attribute lists and 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 specified by management domains. They are applicable for an interim period.

Various forms of O/R addresses are defined, each serving its 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 may also be 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 with numeric keypads.
- *Postal O/R address*: Provides a means of identifying originators and recipients of messages and notifications, for physical delivery.

2.1.1 *Mnemonic O/R address*

This form of O/R address provides addresses that mnemonically identifies a user or a DL relative to the Administration Management Domain (ADMD) through which the user is accessed. At least one of the conditional attributes following the domain name(s) has to be present.

- Country name
- Administration domain name
- [Private domain name]
- [Organization name]
- [Organizational unit name]
- [Personal name]
- [Common name]
- [[Domain defined attributes]]

Note – Attributes in square brackets are conditional. Double square brackets indicate an attribute not belonging to the standard attribute list.

2.1.2 *Terminal O/R address*

This form of O/R address provides a means for addressing a terminal with its network address, conditionally with the country name, the domain name(s), a terminal identifier and domain defined attributes.

- [Country name]
- [Administration domain name]
- [Private domain name]
- Network address
- [Terminal identifier]
- [Terminal type]
- [[Domain defined attributes]]

Note 1 – Attributes in square brackets are conditional. Double square brackets indicate an attribute not belonging to the standard attribute list.

Note 2 – Domain defined attributes shall be present only if the country name and the administration domain name are present.

The network address is composed of digits from the X.121 numbering plan (including escape codes) or the E.163/E.164 numbering plan.

The conditional terminal identifier might be, for example, a telex answerback string or a teletex terminal identifier.

The conditional terminal type might be, for example, a telex, a teletex, a G3 facsimile, a G4 facsimile, an IA5, and a videotex terminal.

2.1.3 *Numeric O/R address*

This form of O/R address provides addresses that can be entered from devices equipped only with numeric keypads. It identifies numerically a user relative to the ADMD through which the user is accessed.

- Country name
- Administration domain name
- [Private domain name]

– Numeric user identifier
– [[Domain defined attributes]]

Note 1 – Attributes in square brackets are conditional. Double square brackets indicate an attribute not belonging to the standard attribute list.

Note 2 – Numeric values are assumed for all attributes.

Note 3 – This form could also be used for a videotex user number.

2.1.4 *Postal O/R address*

This form of O/R address provides for the identification of a user by means of his postal addresss, together with the country name(s), and the domain name(s), and the PD service name through which he is accessed.

See also Recommendation F.415.

Version 1 – Unformatted postal O/R address:
– Physical delivery country name
– Country name
– Administration domain name
– [Private domain name]
– [Physical delivery service name]
– Postal code
– Unformatted postal address

Sufficient address components have to be supplied in the unformatted postal address in order to enable the PD service to route, distribute and deliver the physical message properly.

Version 2 – Formatted postal O/R address:
– Physical delivery country name
– Country name
– Administration domain name
– [Private domain name]
– [Physical delivery service name]
– Postal code
– Set of formatted postal address attributes

There is no defined order in the set of formatted postal address attributes. These attributes are:

– *Postal O/R address components*:
  a) [Physical delivery personal name]
  b) [Physical delivery organization name]
– *Physical delivery address components*:
  a) [Street address]
  b) [P.O. box address]
  c) [Poste restante address]
  d) [Unique postal name]
– *Physical delivery office address components*:
  a) Physical delivery office name
  b) [Physical delivery office number]
  c) [Local postal attribute]
– *Other postal address components*:
  a) [Extension of postal O/R address components]
  b) [Extension of physical delivery address components]

Note – Attributes in square brackets are conditional.

Sufficient attributes have to be provided in order to enable the PD service to route, distribute and deliver the physical message properly.

For the description of formatted postal O/R address attributes see Annex A/F.400 and for the length see § 3.

2.2 *Distribution list names*

In the context of message handling, names of distribution lists (making use of the common name attribute) are used to identify the point of expansion of a message using a distribution list which contains a set of O/R addresses or further distribution list names (see Recommendation F.400).

Care should be taken in the choice of distribution list names to ensure that users are aware that they are addressing a distribution list.

Note – For naming of distribution lists the attribute "Common Name" may be used. Names of distribution lists should clearly indicate their purpose.

2.3 *Directory names*

In the context of message handling a directory name can be used to retrieve the required O/R address from a directory (see Recommendations F.400 and F.500). The directory may be provided by local functions.

3 Length of attributes

The coding is specified in the Recommendations of the X.400 series.

The O/R address shall allow the following information:

- *Country name*

  The Alpha-2 country code listed in Appendix I or the DCC from Recommendation X.121 is used as the numeric country name. Maximum 3 characters.

- *Physical delivery country name*

  The same conditions apply as for country name.

- *Administration domain name*

  Maximum 16 characters. Numeric O/R address form assumes allocation of numeric administration domain names.

- *Private domain name*

  Maximum 16 characters.

- *Physical delivery service name*

  Maximum 16 characters

- *Organization name*

  Maximum 64 characters

- *Organizational unit(s)*

  Maximum 32 characters each

  Note – At least one organizational unit should be supported on the sending side.

- *Personal name*

  Maximum is the sum of the maxima of the parts (64 characters).

  a) Surname – maximum 40 characters.

  b) Given name – maximum 16 characters.

  c) Initials (optional) – maximum 5 characters (for further study).

  d) Generation qualifier (optional) – maximum 3 characters.

- *Distribution list name*

  Maximum of the common name applies.

- *Common name*

  Maximum 64 characters.

– *Domain defined attributes*

Maximum four separate attributes, maximum length for "type" 8 and for "value" 128 characters.

– *Network address*

Maximum 14 + 1 digits, including the prefix (see Recommendation X.121).

Note – The classification and maximum value may change to accommodate other addressing schemes.

– *Terminal identifier*

Maximum 24 characters.

– *Unformatted postal address*

Up to 6 lines with a maximum of 30 characters each. In the case of transit mail the last line is reserved for the name of the country of the final physical destinaton (see Note 1).

– *Formatted postal address*

Formatted postal address attributes

These attributes and their constraints are: (for the description of these attributes see Annex A/F.400)

– *Postal O/R address components* (see Note 2)

Physical delivery personal name (see Note 3)

30 characters (see Note 1)

Physical delivery organization name (see Note 3)

30 characters (see Note 1)

– *Physical delivery address components* (see Note 2)

Street address

30 characters (see Note 1)

P.O. box address

30 characters (see Note 1)

Poste restante address

30 characters (see Note 1)

Unique name

30 characters (see Note 1)

– *Physical delivery office address components*

Physical delivery office name

x characters (see Notes 1 and 4)

Physical delivery office number

y characters (see Notes 1 and 4)

Local postal attributes

z characters (see Notes 1 and 4)

– *Other postal address components*

Extension of O/R address components (see Note 5)

30 characters (see Note 1)

Extension of physical delivery address components (see Note 6)

30 characters (see Note 1)

The overall constraints are 6 lines of attributes with a maximum of 30 characters in each line. In the case of transit mail the last line is reserved for the name of the receiving country of the final physical destination.

Note 1 – The number of characters specified refers to characters to be printed (including spaces).

Note 2 – At least one of the following attributes should be used.

Note 3 – Physical delivery personal name and physical delivery organization name are free form names and have different length from personal name and organization name.

Note 4 – These attributes have to be printed in one line, in some countries together with the postal code. Thus x + y + z is a maximum of 30 characters including the delimiting spaces and the postal code if printed in the same line.

Note 5 – May be used to extend the postal O/R address components.

Note 6 – May be used to extend the physical delivery address components.

4 Principles for the allocation of O/R names and O/R addresses

4.1 The naming authority of the country responsible for administration domain names will ensure the designation of an unambiguous name to each ADMD of message handling services in that country.

4.2 Each ADMD is responsible for the administration of names for private management domains associated with it.

Note – For PRMDs intercommunicating with more than one ADMD, agreement between all the ADMDs concerned is necessary for an unambiguous name of the PRMD.

4.3 Each management domain (MD) is responsible for allocating unambiguous addresses to users below the level of the MD name(s) for the purpose of using message handling services.

4.4 A distribution list only shall be given a name which is clearly indicating to the user its intent. Names or O/R addresses shall only be included in a publicly accessible distribution list when the permission of the owner of the information is given and national rules for security are respected.

5 Use of O/R names

5.1 *General*

With the help of O/R names a user can send messages via the MHS. Users may get support from their user agent in the use of O/R names. The latter is a local matter.

5.2 *Character repertoires*

The character repertoire allowed in O/R names are either printable, numeric or teletex repertoires (for more detail see Recommendation X.402).

The printable character repertoire is shown in Table 1/F.401.

The numeric character repertoire is comprising the digits 0 - 9 and space, and is a subset of the printable character repertoire.

For the teletex repertoire see Recommendation T.61. In general the teletex repertoire may also be used internationally.

All name attributes that may use the teletex repertoire shall, when sent internationally, be conveyed together with the equivalent attribute(s) using the repertoire specified in Table 1/F.401.

The use of an extended character repertoire within a management domain is a local matter.

5.3 *Specific rules*

Rules for postal O/R addresses, see §§ 2 and 3 and Recommendation F.415.

Management domains will not allow O/R names, that differ only by the number of "space" characters, either at the beginning or the end of any of their attributes, to identify different users.

Additionally MDs will not consider an O/R address attribute to identify different users when the attribute contains more than one word separated by one or more "space" characters.

MDs will not allow O/R names, that differ only by small letter/capital letter distinctions, to identify different user.

5.4 *Support of forms of O/R addresses*

Each MHS shall support all the name address forms in the incoming direction for transitting purposes. It is the decision of the management of a domain which name forms are allocated to the users of that domain. In the outgoing direction the originating domain needs to use the name forms the destination domain applies. The way in which names are input by or presented to the subscriber is a local matter.

TABLE 1/F.401

Printable character repertoire for O/R names

Designation	Graphic representation
Capital letters	A, B, ..., Z
Small letters	a, b, ..., z
Digits	0, 1, ..., 9
Space	(space)
Apostrophe	'
Left parenthesis	(
Right parenthesis	)
Plus sign	+
Comma	,
Hyphen	-
Full stop	.
Solidus	/
Colon	:
Equals sign	=
Question mark	?

Note – According to Recommendation X.208 this repertoire is called a Printable String type. All these characters are available in ITA2 (as far as letters are concerned, only in upper or lower case).

6 References

Recommendation F.400	Message handling – System and service overview
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	Messsage 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
Recommendations of the X.400 series	Message handling – System and service overview
Recommendation T.61	Character repertoire and coded character sets for the international teletex service
Recommendations of the X.500 series	The directory – Overview of concepts, models and services
Recommendation F.500	International public directory services
Recommendation X.121	International numbering plan for public data networks
Recommendation E.163	Numbering Plan for the international telephone service
Recommendation E.164	Numbering Plan for the ISDN Era
ISO 3166	Codes for the representation of names of countries

ANNEX A

(to Recommendation F.401)

Abbreviations

ADMD	Administration Management Domain
DCC	Data Country Code
DL	Distribution List
IA5	International Alphabet 5
IPM	Interpersonal Messaging
ITA2	International Telegraph Alphabet 2
MD	Management Domain
MH	Message Handling
MHE	Message Handling Environment
MHS	Message Handling System
MT	Message Transfer
O/R	Originator/Recipient
P.O.	Post Office
PD	Physical Delivery
PRMD	Private Management Domain
RPOA	Recognized Private Operating Agency
UPU	Universal Postal Union

Note – For a glossary of terms see Annex A of Recommendation F.400.

APPENDIX I

(to Recommendation F.401)

List of Alpha-2 country codes

Afghanistan	AF	Bhutan	BT
Albania	AL	Bolivia	BO
Algeria	DZ	Botswana	BW
American Samoa	AS	Bouvet Island	BV
Andorra	AD	Brazil	BR
Angola	AO	British Indian Ocean Territory	IO
Anguilla	AI	British Virgin Islands	VG
Antarctica	AQ	Brunei Darussalam	BN
Antigua and Barbuda	AG	Bulgaria	BG
Argentina	AR	Burkina Faso	BF
Aruba	AW	Burma	BU
Australia	AU	Burundi	BI
Austria	AT	Byelorussian SR	BY
Bahamas	BS	Cameroon	CM
Bahrain	BH	Canada	CA
Bangladesh	BD	Cape Verde	CV
Barbados	BB	Cayman Islands	KY
Belgium	BE	Central African Republic	CF
Belize	BZ	Chad	TD
Benin	BJ	Chile	CL
Bermuda	BM	China	CN

Christmas Islands	CX
Cocos (Keeling) Islands	CC
Colombia	CO
Comoros	KM
Congo	CG
Cook Islands	CK
Costa Rica	CR
Côte d'Ivoire	CI
Cuba	CU
Cyprus	CY
Czechoslovakia	CS
Denmark	DK
Djibouti	DJ
Dominica	DM
Dominican Republic	DO
East Timor	TP
Ecuador	EC
Egypt	EG
El Savador	SV
Equatorial Guinea	GQ
Ethiopia	ET
Faeroe Islands	FO
Falkland Islands (Malvinas)	FK
Fiji	FJ
Finland	FI
France	FR
French Guiana	GF
French Polynesia	PF
French Southern Territories	TF
Gabon	GA
Gambia	GM
German Democratic Republic	DD
Germany, Federal Republic of	DE
Ghana	GH
Gibraltar	GI
Greece	GR
Greenland	GL
Grenada	GD
Guadeloupe	GP
Guam	GU
Guatemala	GT
Guinea	GN
Guinea-Bissau	GW
Guyana	GY
Haïti	HT
Heard and McDonald Islands	HM
Honduras	HN
Hong Kong	HK
Hungary	HU
Iceland	IS
India	IN
Indonesia	ID
Iran, Islamic Republic of	IR
Iraq	IQ
Ireland	IE
Israel	IL
Italy	IT
Jamaica	JM
Japan	JP
Jordan	JO
Kampuchea, Democratic	KH
Kenya	KE
Kiribati	KI
Korea, Democratic People's Republic of	KP
Korea, Republic of	KR
Kuwait	KW
Lao People's Democratic Republic	LA
Lebanon	LB
Lesotho	LS
Liberia	LR
Libyan Arab Jamahiriya	LY
Liechtenstein	LI
Luxembourg	LU
Macau	MO
Madagascar	MG
Malawi	MW
Malaysia	MY
Maldives	MV
Mali	ML
Malta	MT
Martinique	MQ
Marshall Islands	MH
Mauritania	MR
Mauritius	MU
Mexico	MX
Micronesia	FM
Monaco	MC
Mongolia	MN
Montserrat	MS
Morocco	MA
Mozambique	MZ
Namibia	NA
Nauru	NR
Nepal	NP
Netherlands	NL
Netherlands Antilles	AN
Neutral Zone (between Saudia Arabia and Iraq)	NT
New Caledonia	NC
New Zealand	NZ
Nicaragua	NI
Niger	NE
Nigeria	NG
Niue	NU
Norfolk Island	NF
Northern Mariana Islands	MP
Norway	NO
Oman	OM
Pakistan	PK
Palau	PW
Panama	PA
Papua New Guinea	PG

Paraguay	PY
Peru	PE
Philippines	PH
Pitcairn	PN
Poland	PL
Portugal	PT
Puerto Rico	PR
Qatar	QA
Réunion	RE
Romania	RO
Rwanda	RW
St. Helena	SH
St. Kitts-Nevis	KN
Saint Lucia	LC
St. Pierre and Miquelon	PM
Saint Vincent and the Grenadines	VC
Samoa	WS
San Marino	SM
Sao Tomé and Principe	ST
Saudi Arabia	SA
Senegal	SN
Seychelles	SC
Sierra Leone	SL
Singapore	SG
Solomon Islands	SB
Somalia	SO
South Africa	ZA
Spain	ES
Sri Lanka	LK
Sudan	SD
Suriname	SR
Svalbard and Jan Mayen Islands	SJ
Swaziland	SZ
Sweden	SE
Switzerland	CH
Syrian Arab Republic	SY
Taiwan, Province of China	TW
Tanzania, United Republic of	TZ
Thailand	TH
Togo	TG
Tokelau	TK
Tonga	TO
Trinidad and Tobago	TT
Tunisia	TN
Turkey	TR
Turks and Caicos Islands	TC
Tuvalu	TV
Uganda	UG
Ukrainian SSR	UA
United Arab Emirates	AE
United Kingdom	GB
United States	US
United States Minor Outlying Islands	UM
Uruguay	UY
USSR	SU
Vanuatu	VU
Vatican City State (Holy See)	VA
Venezuela	VE
Viet Nam	VN
Virgin Islands, U.S	VI
Wake Islands	WK
Wallis and Futuna Islands	WF
Western Sahara	EH
Yemen	YE
Yemen, Democratic	YD
Yugoslavia	YU
Zaire	ZR
Zambia	ZM
Zimbabwe	ZW

Source: ISO 3166

Current edition (1981 plus amendments up to 1987) at time of printing. The latest published edition from ISO should be applied.

MESSAGE HANDLING SERVICES: THE PUBLIC MESSAGE TRANSFER SERVICE

The establishment in various countries of message handling services in association with public networks creates the need to produce Recommendations covering the aspects of public message handling services.

The CCITT,

considering

(a) the need for public message handling services;

(b) the strategic and commercial importance of standardization of message handling services;

(c) the urgent need for intercommunication arrangements for existing telematic services, and other services with public message handling services;

(d) the need for a clear distinction between the responsibilities to be allocated to service providers and those of subscribers and/or users;

(e) the need for establishing international compatibility between different messaging systems;

(f) the growth of the installed base of terminals and personal computers with the ability to access message handling systems;

(g) that several F series Recommendations describe public message handling services;

(h) that certain X and T series Recommendations cover relevant aspects of systems used for the provision of messaging services,

unanimously declares

the view that the requirements specified in this Recommendation should be applied for the provision of the public message transfer service internationally.

CONTENTS

1 Purpose and scope

1.1 *General*

This Recommendation specifies the general, operational and quality of service aspects of the public international message transfer service.

This type of message handling service is an international telecommunication service offered by Administrations, enabling subscribers' user agents to submit standardized classes of messages to message transfer agents for their transfer to another message transfer agent in the same Administration's domain, in another Administration's domain, or to private domains, via telecommunication networks using store and forward techniques.

The message transfer service also may transfer messages submitted through a message store, and delivered to a message store, and to and from access units to other services.

Locally provided functions, for which communication with other user agents or message transfer agents is not required, are nor covered by CCITT Recommendations.

The message transfer (MT) service enables subscribers to request a variety of features to be performed during the transfer of messages.

Some features are inherent in the basic MT service. Other non-basic features may be selected by the subscriber, either on a per-message basis, or for an agreed contractual period of time, if they are provided by Administrations.

Elements of service belonging to the basic message transfer service and essential optional user facilities are to be made available internationally by Administrations.

MT service may be provided using any physical network. MT service may be offered separately or in combination with various telematic or data communication services. It can be obtained by making appropriate arrangements.

Technical specifications and protocols, to be used in the MT service are defined in the X.400 series of Recommendations.

The service definition is contained in § 2. Sections 3 and 4 describe the operation of the service and quality of service, and network requirements are given in § 5.

1.2 *Message handling systems used in the provision of MT service*

1.2.1 *1984 implementations*

This Recommendation assumes that the message handling systems implemented to provide the service outlined herein are based on the 1988 version of the X.400 series of technical Recommendations. It is recognized however that for some time after the publication of this Recommendation, the majority of implementations of MT service will be based on the 1984 X.400 series of Recommendations. Administrations are encouraged to adopt the latest CCITT Recommendations; however, in the interim, they may make use of this Recommendation with 1984 implementations as outlined below.

1.2.2 *Elements of service*

The elements of service available for message handling services are listed and classified in Recommendation F.400. Annex B/F.400 provides a list of all the elements of service (called Service Elements in 1984) for MT service from the 1984 X.400 Recommendation. In addition the classifications of each element of service, as they were in 1984 in Recommendation X.401, are shown. In the 1988 X.400 Recommendation, there are many new elements of service representing new functionality that were not present in 1984. Most of these have been classified as additional, meaning that they do not have to be supported, hence the 1984 implementations can make use of this service Recommendation in most cases. Other differences between 1988 and 1984 are of two types, new elements of service that are classified as essential, and old (meaning 1984) elements of service that have been re-classified as essential for 1988. Annex C of Recommendation F.400 lists both the new elements of service in 1988 as well as changes in classification to any 1984 elements of service. In both cases to allow for 1984 implementations to be used for the provision of pubic MT service as described in this Recommendation, a grace period of 8 years is provided for Administrations to upgrade their implementations in this respect to the 1988 technical Recommendations.

1.2.3 *Name forms*

The specifications of the name forms in the 1988 Recommendations have been enhanced and postal O/R addresses have been added. The name forms and the mandatory components of the 1984 Recommendations have their equivalence in the new framework and are aligned in principle.

1.2.4 *Interworking*

In order to protect the investment of Administrations who have implemented 1984 systems for the provision of MT service, 1988 ADMD implementations must be able to interwork to 1984 ADMDs as outlined in Recommendation X.419, Annex B.

Interworking from 1988 ADMDs to 1984 PRMDs is a national matter.

2 MT service

2.1 *General service requirements*

2.1.1 The fundamental ability of the MT Service is to provide for the transfer of messages submitted by other services subscribing to the MT service. These other services may submit messages from their user agents, if they are services that follow the X.400 series of Recommendations. Services may also access the MT service from standardized access units. Messages may also be transferred to and from message stores. The access units and message stores are not part of the MT service. Conversion of messages when different codings and other formats are used may be provided by the MT service.

2.1.2 The public MT service will be provided by Administrations using systems that conform to the X.400 series Recommendations.

Management domains (MDs) are defined for the purpose of responsibilities boundaries. The MD managed by an Administration is called an Administration Management Domain (ADMD). The MD managed by an organization is called a Private Management Domain (PRMD).

2.1.3 International exchange of messages are performed between administation management domains through CCITT standardized public data transmission services. Each Administration will designate one or more MTAs in its management domain as international access points to the MT service.

2.1.4 Different classes of messages may be exchanged through this service. Some classes of messages may be standardized by CCITT Recommendations, such as F.420. Other classes of messages may also be transferred, provided that the format adheres to the appropriate X.400 series or Recommendations.

2.1.5 An Administration may provide different methods of access to the MT service. The possible methods are:

1) from a subscribing service's user agent, message store, or access unit;

2) from an MTA in a private management domain.

2.1.6 Each Administration is responsible for the national access to its management domain.

2.1.7 The characteristics of the direct interfaces to the MT service, or between a private domain and the MT service are a national matter, although they should generally conform to the X.400 series of Recommendations. Interworking with postal systems, or other physical delivery systems, should be in accordance with F.415.

2.1.8 The national implementation of the MT service may provide intercommunication of subscribing services with other telematic services such as telex, teletex, facsimile and videotex. When implemented, the interface between the MT service and the other services shall be according to relevant CCITT Recommendations. Intercommunication may also be provided to a physical delivery system.

2.1.9 As the service is providing indirect communication, cases of non-delivery of the message to the intended recipient may occur. The MT service provides for non-delivery notification and, as an optional user facility, for delivery notification.

2.1.10 Due to the intermediate storage of the message, the service may provide conversion optional user facilities: speed, access procedures, networks, and coding of message contents.

2.1.11 The message belongs to the originator until delivery has taken place. After delivery the message belongs to the recipient.

2.1.12 Where sender and recipient have different and conflicting requirements, the sender's requirements shall take precedence (e.g., content type conversion or redirection control).

2.1.13 Management domains shall relay messages even if some additional optional user facilities are not supported by that domain.

2.2 *Message transfer service features*

2.2.1 *Introduction*

Recommendation F.400, § 19, defines elements of service which are available in the MT service and are classified as either belonging to the basic service or as MT optional user facilities. Elements of service comprising the basic MT service are inherently part of the service, and are always provided and available. The optional user facilities that are classified as essential are always provided and those classified as additional may be available nationally or internationally on the basis of bilateral agreement.

In the MT service there is the following grouping of elements of service:

1) basic service which corresponds with the basic elements of service listed in Table 4/F.400;

2) optional user facilities, which correspond to the MT optional user facilities listed in Table 5/F.400.

Basic features are inherent in the service. Optional user facilities may be selected on a per-message basis or for an agreed contractual period of time.

2.2.2 *The basic message transfer service*

The basic MT service shall be implemented according to the requirements of CCITT Recommendation X.411. The basic MT service enables UAs to access and be accessed by the MTS in order to exchange messages. Each message is assigned a unique message reference identification. If a message cannot be delivered, the originating UA is informed. To facilitate meaningful communication, a UA may specify the types of encoded information that can be contained in messages delivered to it. The content type, the original encoded information types, the time of submission and delivery and whether conversion occurred are indicated for each message. The elements of service comprising the basic MT service are listed in Recommendation F.400, Table 4/F.400.

2.2.3 *Optional user facilities in the MT service*

Two classes of optional user facilities are available in the MT services. The first class is selectable on a per-message basis. The second class may be provided to the subscribing service when agreed to over a contractual period of time. The classes are described and cited in Recommendation F.400 (§ 19.3, and Table 5/F.400) and are available in the service based on the MT service.

2.2.4 *Naming and addressing*

Naming and addressing as used in the MT service is described in overview in Recommendation F.400, § 12. The rules for naming and addressing in an Administration Management Domain are given in Recommendation F.401.

3 Operation of the service

3.1 *General*

3.1.1 The MT service provides that messages can be sent, transferred, delivered and received using fully automatic procedures.

Manual delivery of messages can be provided in the case of interworking with postal systems, and is described in Recommendation F.415.

3.1.2 Messages are prepared by subscribers services User Agents/Access Units or by User Agents/Access Units in other management domains.

3.1.3 Each Administration providing the MT service should validate its subscribers identities, at the time of access. It should also validate the identity of other Management Domains at their points of access.

3.1.4 Connectivity of the MT service to message transfer in private management domains, which will allow users of these systems to exchange messages, is desirable. This is recognized to be a national matter. If these interconnections are provided, they should take place between management domains in accordance with CCITT Recommendations.

3.1.5 When implicit conversion is provided by the Administration via the message transfer service, the message will be converted if necessary, unless prohibited by the originator. The conversion will be in accordance to the rules specified in Recommendation X.408.

3.2 *Message transfer*

Message transfer is initiated when a message is received from a User Agent/Message Store or access unit. Delivery is attempted to the address of the message. The body part of the message will be transferred in the form in which it was received unless conversion has been performed.

The results of the transfer attempt may be conveyed by two notifications.

- non-delivery notification;
- delivery notification.

Delivery notification may be given to the originating domain by the destination domain to indicate successful delivery. This delivery notification should be provided if requested.

Non-delivery notification is automatically originated by the MTS, while delivery notification will be generated by the recipients MTA on request of the originator. If non-delivery notification is prevented, and delivery notification is not requested, no notification is possible. In the case of a message to a teletex terminal, (auto) receipt notification may be returned by the TTXAU.

4 Quality of service

4.1 *Message status*

The unique identification of messages conforming to the requirements of CCITT X.400 series Recommendations enables the system to provide information about e.g., the status of an IP-message or other class of message.

In the event of system failure all accepted and non-delivered messages should be traceable. If messages cannot be delivered, the originator must be informed by a non-delivery notification.

4.2 *Responsibility for messages*

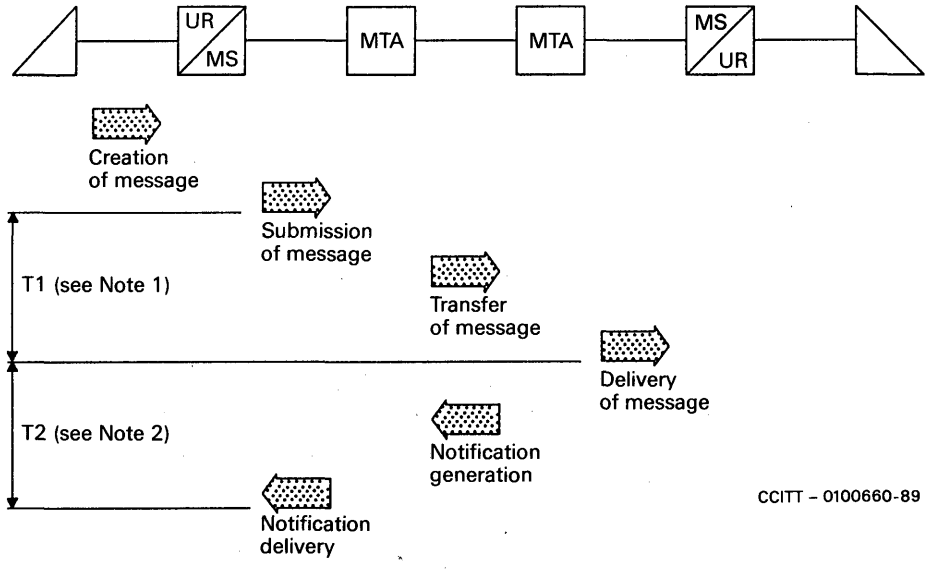
The subscribers to the service using the MTS are responsible for the messages in their User Agents/ Message Stores. The service using the MT service is responsible for the transfer between the UAs/MSs in that service and the MT service.

The Administration providing the MT service is responsible for the message transfer and the optional user facilities performed within its management domain and for messages coming from or directed to private management domains connected to its management domain, unless other national regulations apply. In international interconnection of ADMDs, the responsibility to deliver passes from managements domains with the message.

Administrations should provide assistance to their subscribers, with regard to status and tracing of non-delivered messages.

Note – The international implications of this are for further study.

4.3 *Model of delivery and notification times* (see Figure 1/F.410)



T1 Delivery time

T2 Delivery notification

Note 1 - Starting time of T1 corresponds to the submission time stamp indication.
Ending time of T1 corresponds to the delivery time stamp indication.

Note 2 - Starting time of T2 corresponds to the delivery time stamp indication.
Ending time of T2 is the time that the delivery notification is made available to the user through the UA or MS.

FIGURE 1/F.410

Delivery and notification time model

4.4 *Message transfer time targets*

The recipient ADMD should force non-delivery notification if it has not been able to transfer the message to the receiving UA before x hours after submission to the originating MTA (or after date and time indicated for deferred delivery), the value of x being dependent on the grade of delivery requested by the originator as shown in Table 1/F.410.

TABLE 1/F.410

Grade of delivery	95% delivered before	Non-delivery forced after *x*
Urgent	0.75 hours	4 hours
Normal	4.0 hours	24 hours
Non-urgent	24.0 hours	36 hours

Note – Intercommunication with PRMDs is not included in the calculation of the time targets.

To be able to meet these time targets, a message has to transit a transitting ADMD within y hours, the value of y being dependent on the grade of delivery requested by the originator as shown in Table 2/F.410.

TABLE 2/F.410

Grade of delivery	95% transitted before *y*
Urgent	0.45 hours
Normal	2.5 hours
Non-urgent	14.5 hours

Note 1 – Time Targets assume that receiving UA is continuously available and excludes cases of Hold for Delivery.

Note 2 – Intercommunication with PRMDs is not included in the calculation of the time targets.

4.5 *Delivery notification time targets*

Non-delivery notifications or requested delivery notifications should be returned on a per-recipient basis, in order not de delay notifications for those messages in a multi-addressed message which have already been delivered, to enable the originating management domain either to return per-recipient notifications or to batch notifications to its subscribers (see Table 3/F.410).

TABLE 3/F.410

Type	95% returned before
ND-notification	0.75 hours
D-notification	0.75 hours

Note – Time Targets assume that receiving UA is continuously available and excludes cases of Hold for Delivery.

4.6 *Error protection*

Error protection on transmission is provided by the MHS and underlying protocols used in the provision of the MT service.

4.7 *Availability of service*

In principle the MT service should be available continuously. User agents or message stores connected to the MT service should be available for submission or delivery continuously (unless hold for delivery is invoked).

4.8 *Minimum storage capacity*

The storage capacity of the message transfer agent shall be sufficient to provide a high grade of service.

Note – This is for further study.

5 Network requirements

5.1 *General*

The MT service is network independent, that is, the basic service and the essential optional user facilities are provided independently of the type of network used for service access. Additional optional user facilities chosen by an Administration to offer may vary.

5.2 *Network requirements for international interconnection*

For an interim period (8 years) in the interest of ease of interconnection of the public international message transfer service between Administrations public packet switching connections shall be used. This does not preclude Administrations from using different means for this interconnection on a bilateral basis.

5.3 *Network requirements for service access*

Access to the public message transfer service is a national matter.

6 Use of the MT service within CCITT defined telematic services

See relevant F series Recommendations.

ANNEX A

(to Recommendation F.410)

Abbreviations

The following abbreviations are used in this Recommendation.

A	Additional Optional User Facility
ADMD	Administration Management Domain
E	Essential Optional User Facility
IP	Interpersonal
MD	Management Domain
MHS	Message Handling System
MS	Message Store
MT	Message Transfer
MTA	Message Transfer Agent
MTS	Message Transfer System
PDS	Physical Delivery System
PRMD	Private Management Domain
TTXAU	Teletex Access Unit
UA	User Agent

Note 1 – For a glossary of terms see Annex A of Recommendation F.400.

Note 2 – For references see Recommendations F.400 and F.401.

ANNEX B

(to Recommendation F.410)

MT elements of service for 1984 systems

Element of service	Classification		
	Basic	Optional	
		Per message	Contractual
Access management	X		
Alternate recipient allowed		E	
Alternate recipient assignment			A
Content type indication	X		
Conversion prohibition		E	
Converted indication	X		
Deferred delivery		E	
Deferred delivery cancellation		E	
Delivery notification		E	
Delivery time stamp indication	X		
Disclosure of other recipients		E	
Explicit conversion		A	
Grade of delivery selection		E	
Hold for delivery			A
Implicit conversion			A
Message identification	X		
Multi-destination delivery		E	
Non-delivery notification	X		
Original encoded information types indication	X		
Prevention of non-delivery notification		A	
Probe		E	
Registered encoded information types	X		
Return of content		A	
Submission time stamp indication	X		

MESSAGE HANDLING SERVICES: INTERCOMMUNICATION WITH PUBLIC PHYSICAL DELIVERY SERVICES

The establishment in various countries of message handling services in association with public networks creates the need to produce Recommendations covering the aspects of public message handling services.

The CCITT,

considering

(a) The need for public message handling services;

(b) the strategic and commercial importance of standardization of message handling services;

(c) the urgent need for intercommunication arrangements for existing telematic services, and other services with public message handling services;

(d) the need for a clear distinction between the responsibilities to be allocated to service providers and those of subscribers and/or users;

(e) the need for establishing international compatibility between different messaging systems;

(f) the growth of the installed base of terminals and personal computers with the ability to access message handling systems;

(g) that several F series Recommendations describe public message handling services;

(h) that certain X and T series Recommendations cover relevant aspects of systems used for the provision of messaging services;

(i) that there is a requirement for delivery of messages from message handling services in physical form to postal addresses;

unanimously declares

the view that the requirements specified in this Recommendation should be applied for the provision of intercommunication between public message handling services and public physical delivery services internationally.

CONTENTS

1 Introduction

This Recommendation specifies the general, operational and quality of service aspects of intercommunication between public message handling (MH) services and public physical delivery (PD) services.

This intercommunication may be offered by Administrations, enabling subscribers to send messages to one or more recipients though telecommunications means for final delivery in physical form through a PD service. The postal services are general examples of public PD services.

The general principles of intercommunication between MH services and PD services are overviewed in Recommendation F.400, and as a generic capability of the message transfer (MT) service in Recommendation F.410.

The capabilities described in this Recommendation cover message transfer (MT) and interpersonal messaging (PM) service intercommunication with PD services.

The output media addressed at this time is hard-copy; other forms of physical delivery media are for further study.

The terms used in this Recommendation are defined in Recommendation F.400.

Technical specifications and protocols to be used for MH/PD service intercommunication as covered in this Recommendation are defined in the X.400 series Recommendations.

2 Scope

The model for MH/PD service intercommunication as covered in this Recommendation is shown in Figure 1/F.415. The actual provisions of PD services are not covered in this Recommendation.

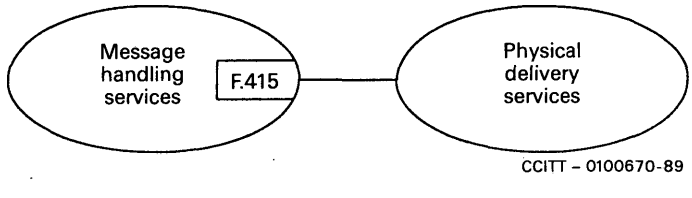


FIGURE 1/F.415

Model for MH/PD service intercommunication

3 Features

3.1 *General description*

The MH/PD intercommunication provides MH users with a variety of facilities to be performed in the process of physical rendition, physical transport, and physical delivery of messages. The elements of service available to originating users are grouped into specific categories as shown in Table 1/F.415.

TABLE 1/F.415

MH/PD elements of service

Category	Elements of service	F.400 Ref.
Physical delivery request	Requested delivery method	B.76
Modes of physical transport and delivery	Ordinary mail	B.53
	Special delivery	B.81
	EMS (express mail service)	B.28
	Counter collection	B.16
	Counter collection with advice	B.17
	Delivery via Bureaufax service	B.23
Registrations	Registered mail	B.70
	Registered mail to addressee in person	B.71
Physical delivery notifications	Undeliverable mail with return of physical message	B.91
	Physical delivery notification by PDS	B.58
	Physical delivery notification by MHS	B.57
Physical forwarding	Physical forwarding allowed	B.59
	Physical forwarding prohibited	B.60
	Request for forwarding address	B.75
Physical rendition capabilities	Basic physical rendition	B.7
	Additional physical rendition	B.2

The definition and classification of MH/PD elements of service are found in Recommendation F.400; base elements of service and optional user facilities are defined. Base capabilities are inherent to the MH/PD service intercommunication and have to be made available internationally by all Administrations supporting this intercommunication. Optional user facilities are selectable by the originator on a per-recipient basis. These are classified as either essential or additional. Essential optional user facilities shall be made available internationally by all Administrations. Additional optional user facilities may be made available by some Administrations for national use and internationally on the basis of bilateral agreement.

3.2 *Application*

All MH/PD elements of service apply on a per-recipient basis.

Various combinations of elements of service are possible. For example, the elements of service category physical delivery notifications are useable with all modes of physical transport and delivery, with registrations and with physical forwarding categories.

The elements of service submission time stamp and delivery time stamp also apply to MH/PD service intercommunication although they are not listed. These are MH elements of service whose definitions include MH/PD intercommunication.

In all cases of physical delivery, it is highly desirable that the originator provide a postal O/R address for PD notifications to be sent by PDS, particularly when these are explicitly requested. To facilitate this, the originating UA could prompt the originator for this information or obtain it from a directory.

Optional user facilities selectable by originating users affecting physical delivery are rendered on the physical message above the recipient's address visible through the window of the envelope to ensure that the proper handling procedures are taken in the PDS. Details of this are described in Annex B.

In the case where the physical message cannot be delivered, it is returned to the originator, depending on the options selected and on national regulations, firstly as a vehicle to carry the non-delivery notification, and secondly to inform the originator on what has happened to the message. Notifications include undeliverable mail diagnostics as defined in Annex C.

Where more than one notification is to be returned to the originator, these are returned together at the farthest delivery point. For example, physical forwarding and physical delivery notification are generated as a combined notification after delivery.

Where the recipient's forwarding address is returned, based on the originator's request, it is returned in the form of a postal address, as defined in Recommendation F.401.

The element of service additional physical rendition is meant to establish generic place holders for use under bilateral agreements and possible future standardization.

The actual methods of physical rendition, routing, and delivery used by Administrations may vary.

4 Physical rendition

4.1 *Basic rendition capabilities*

The PDAU and associated PDS provide the capabilities for rendition, routing, transport, and delivery of physical messages based on inherent and user selected facilities as defined by the elements of service.

Details of the basic physical rendition (hard copy) process are provided in Annex B.

4.2 *Rendition of IPM headers*

In the case of IP-messages, heading information is printed on the physical message. The language selected is based on either the language indication element of service (provided that this is supported in the receiving country) or the default national language(s) of the receiving country. Originators and/or originating UAs are encouraged to specify the language.

4.3 *Additional rendition capabilities*

Additional physical rendition capabilities of the PDAU are for further study, but may be provided by Administrations on the basis of bilateral agreements.

Possible additions include:

- use of extended character sets;
- ability to select pre-encoded information (such as digitized logos and signatures) for rendition;
- support of other encoded information types.

5 Naming and addressing

Naming and addressing in message handling services is described in Recommendation F.400.

For the purpose of physical delivery, the recipient of the physical message is identified by means of a postal O/R address as defined in Recommendation F.401.

PD country name and country name would normally be identical, except in the case of transit mail. This occurs when a message is destined to a country which does not offer MH/PD service intercommunication; the message would then be routed and printed in the nearest country (or another country based on established agreements), and subsequently physically delivered to the final destination.

A postal code is required for the routing of the MHS message to the proper PDAU. It may default to unspecified if no postal code exists.

Two versions of postal O/R address are provided to allow:

a) the use of the postal address as it commonly exists (Version 1 – unformatted postal O/R address);

b) for further automatic routing within the PDS (Version 2 – formatted postal O/R address).

Administrations should support both versions of the Postal O/R Address, and should encourage MH users to use the Formatted Postal O/R Address (Version 2).

Users should be made aware that sufficient address information about the recipient and final destination has to be provided in either version of the postal O/R address in order to enable the PDS to route, transport and deliver a physical message properly.

In terms of formatted postal address attributes, these generally comprise:

- one attribute of O/R address componets;
- one attribute of physical delivery address components; and
- the required set of attributes of physical delivery office address components.

The postal O/R address is also used to supply the postal address of the originator of a physical message.

Examples of postal O/R addresses are provided in Appendix I.

6 Quality of service

6.1 *Service objectives*

Administrations are responsible for providing the service requested by the originator. In the event of failure, it would be beneficial if accepted and non-delivered messages would be traceable and the originator informed.

6.2 *Message status*

Administrations could provide assistance to their subscribers with regards to delivery status. The extent to which provisions are made for support of status and tracing of messages is a national matter.

6.3 *Delivery and notification times model*

Figure 2/F.415 depicts a model of delivery and notification times relative to MH/PD service intercommunication.

The meaning of times "Tn" in Figure 2/F.415 are defined as follows:

T1 = delivery time of MH message

1) Start time corresponds to the submission time stamp.

2) End time corresponds to the delivery time stamp.

T2 = delivery notification of MH message

1) Start time corresponds to the delivery time stamp.

2) End time corresponds to the time that the MH notification is made available to the user through the UA or MS.

T3 = physical delivery notification by MHS

1) Start time corresponds to the time at which the physical delivery notification by MHS has been generated.

2) End time corresponds to the time that the physical delivery notification by MHS is made available to the user through the UA or MS.

Ta = physical handling

1) Start time corresponds to the delivery time stamp.

2) End time corresponds to the time at which the physical message is delivered to the recipient.

Note – Physical handling includes physical rendition, transport, and delivery.

Tb = generation of physical delivery notification by MHS

1) Start time corresponds to the time at which the physical message is delivered to the recipient.

2) End time corresponds to the time that the physical delivery notification by MHS is generated in the MHS.

Tc = physical delivery notification by PDS

1) Start time corresponds to the time at which the physical message is delivered to the recipient.

2) End time corresponds to the time that the physical delivery notification by PDS is delivered to the originator.

Note – This time includes the generation of the physical delivery notification by PDS.

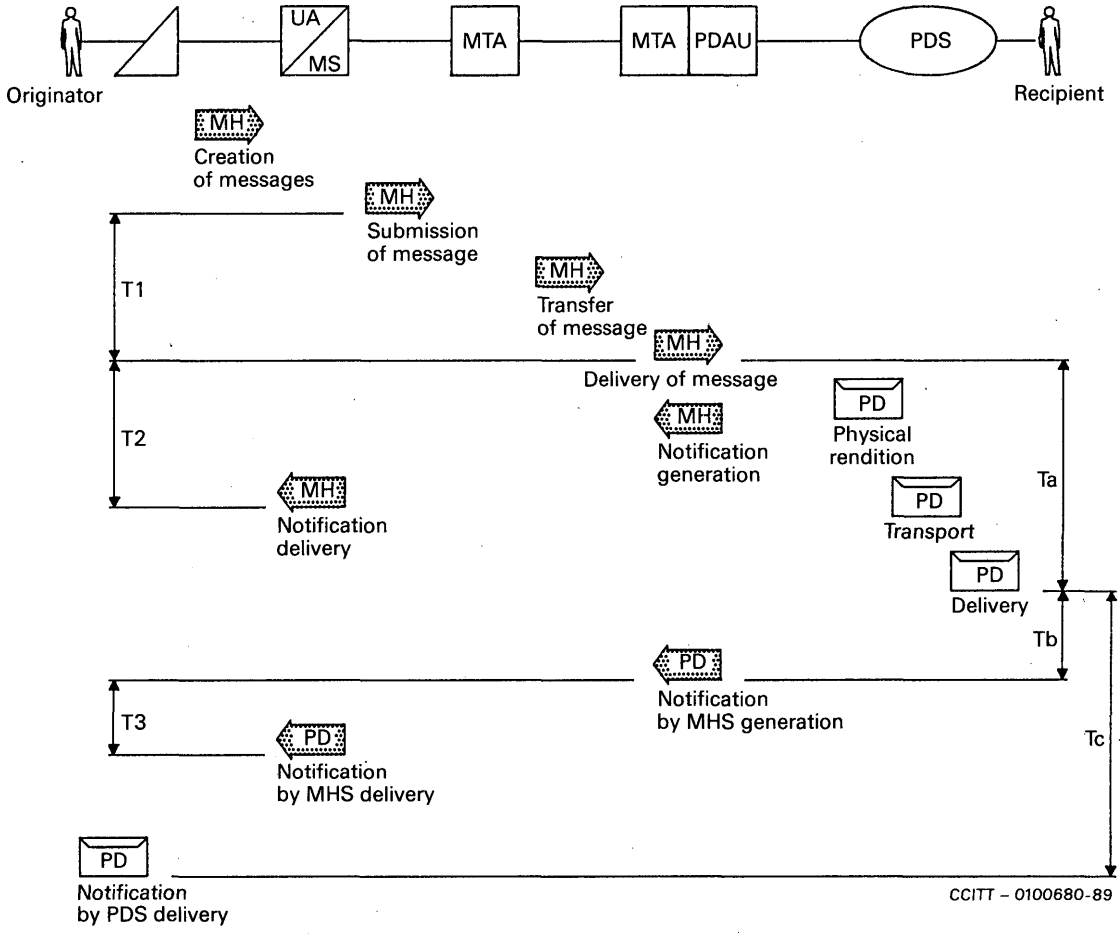


FIGURE 2/F.415

MH/PD delivery and notification times model

6.4 *Time targets*

Time targets for MH (T1, T2, T3 in Figure 2/F.415) are specified in Recommendations F.410 and F.420. In addition, times for physical handling (Ta, Tb, Tc in Figure 2/F.415) need to be considered. These time targets are not specified in this Recommendation but could be defined in the MH/PD service profile table described in § 7.

Time targets for physical handling are dependent on the modes of physical transport and delivery requested by the originator and on the modes offered by the destination Administration.

6.5 *Responsability for messages*

From the point of view of MH/PD service intercommunication, responsibility for physical delivery starts at the point where the MTA passes the message to the PDAU. Responsibility for messages prior to that belongs in MHS.

Delivery through a specific PDS is a user option. If the user does not specify a certain PDS, messages are handled by the PDS associated with the MH domain. If there is more than one PDS, the traffic is routed based on administrative agreements.

Although MH messages with incomplete physical routing data may cause problems or delays, service providers should accept such messages in at least one gateway station and arrange for further routing as appropriate.

The MHS could check whether the requested elements of service and rendition capabilities are compatible with those offered by the destination MTA/PDAU and PDS. If this check is positive, the message is accepted by the MTA/PDAU which generates the delivery time stamp indication. This time stamp appears in the field service data as detailed in Annex B.

6.6 *Handling of incompatibilities*

If MH messages are destined for a MH/PD service which does not offer the requested elements of service, or additional capabilities, the messages should be transferred to another suitable MH/PD service in the same management domain, or in another management domain (another country in the case of transit mail), based on established agreements.

Another method for handling incompatible messages is to replace requested additional optional elements of service and printing capabilities by the best comparable service and to inform the originator, and if necessary also the recipient, about the chosen alternatives.

If neither of these methods of handling incompatibilities are possible the MTA/PDAU shall reject the MS message and initiate a non-delivery report. The non-delivery report shall inform the originating UA of the reasons for rejection of a message.

7 User information and support

When possible, the correctness and completeness of the physical routing data could be checked and flagged to the originator at origination.

To prevent incompatible international MH messages from being sent, the international community of users should be provided with all necessary information on the service provisions of MTA/PDAUs and PDS.

This information is to be defined in MH/PD service profile tables and is to be provided either in hard-copy form or preferably in electronic form.

These MH/PD profile tables will contain all the information required for routing traffic as well as information concerning additional optional user facilities and time targets provided by the destination Administration.

Note – The specification of the type of information to be contained in the MH/PD service profile tables is for urgent further study.

Each Administration participating in this intercommunication should apply information required for the MH/PD service profile tables to the ITU secretariat, either directly or through the International Bureau of the UPU. All subsequent amendments should be communicated by the Administrations without delay.

The ITU General Secretariat will publish the MH/PD service profile tables containing the information received from Administrations. Subsequent amendments are published in the ITU Operational Bulletin.

Note – The use of Probe or directory enquiries for originators to obtain information on a MH/PD services prior to sending a message are for further study.

8 Network requirements

Provision of MH/PD services is network independent. Basic service and optional user facilities are provided independently of the type of network used for service access.

9 Tariff and accounting considerations

Tariff and accounting considerations applicable to the provisions of MH/PD services are for further study by CCITT and the UPU.

The following elements of accounting components may need to be studied:

- a basic charge component for the use of MH/PD service intercommunication (for ordinary mail delivery);
- additional charge components based on the request for optional user facilities;
- charge components based on the size of the message (number of pages) and the distance the message travels;
- charge components for the establishment and maintenance of address lists and other information which is stored on behalf of a user;
- charge components for additional physical rendition, such as the registration and storage of graphics (logo, signature).

ANNEX A

(to Recommendation F.415)

Abbreviations

EOS	Elements of Service
IA5	International Alphabet 5
IP	Interpersonal
IPM	Interpersonal Messaging
IRV	International Reference Version
ISO	International Organization for Standardization
ITU	International Telecommunications Union
MH	Message Handling
MHS	Message Handling Systems
MS	Message Store
MT	Message Transfer
MTA	Message Transfer Agent
O/R	Originator/Recipient
PD	Physical Delivery
PDAU	Physical Delivery Access Unit
PDS	Physical Delivery System
UA	User Agent
UPU	Universal Postal Union

Note 1 – For a glossary of terms see Annex A of Recommendation F.400.

Note 2 – For references see Recommendations F.400 and F.401.

Note 3 – Administration is used in short form to indicate a Telecommunication Administration, a Recognized Private Operating Agency, and in the case of Message Handling Services intercommunication with Physical Delivery Services, a Postal Administration.

ANNEX B

(to Recommendation F.415)

Physical rendition details

B.1 *Basic rendition capabilities*

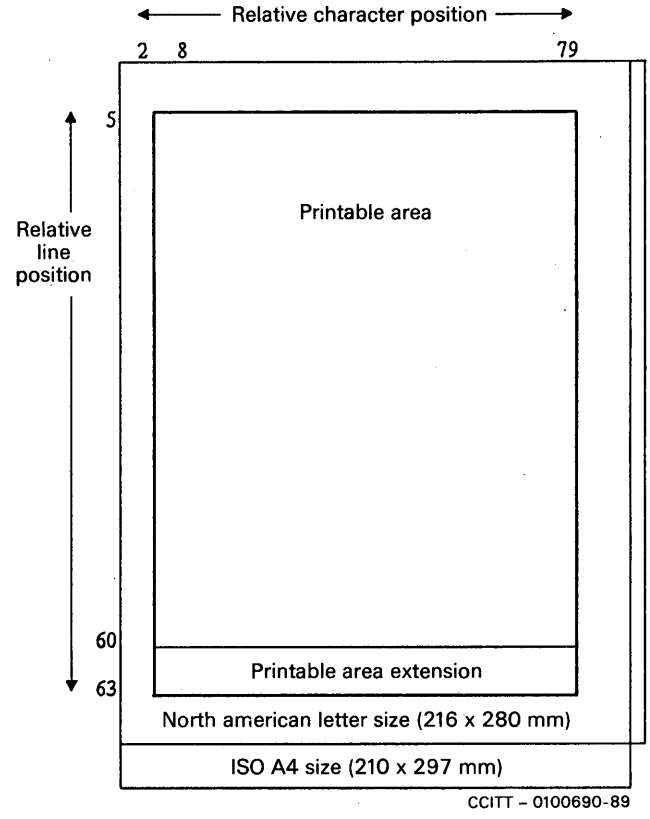
Messages destined for physical delivery are conveyed by the message transfer service and routed to an MTA/PDAU, the link between MHS and PDS. The MTA/PDAU provides the capabilities for the physical rendition based on the originator's message(s) and selected facilities.

The physical message consists of a window envelope and a limited number of pages with imprinted information. Information is printed as information fields as follows:

- letter-head information;
- indication of requested elements of service;
- postal address of the recipient;
- text of the message; and
- service data.

B.2 *Printable area*

The information is printed in vertical orientation in an area which is the common printablea area of the 297 mm x 210 mm (ISO A4) and 280 mm x 216 mm (North American letter size) formats, as specified in Figure A-2/T.60 (dotted area). This area is extended by three additional lines down to the bottom edge which is easily possible with both formats. Figure B-1/F.415 shows the printable area.



Note - For illustrative purposes only - not to scale. Relative positions based on 10 characters and 6 lines per inch.

FIGURE B-1/F.415

Printable area

B.3 *Paper characteristics*

The choice of an appropriate paper type is a national matter as long as the printable area can be accommodated.

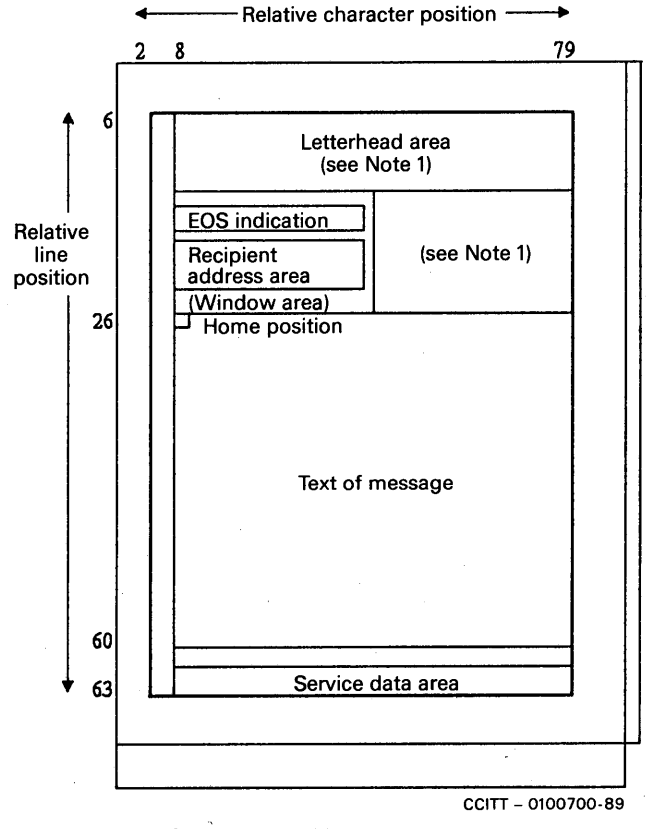
Information should be printed on plain light paper and on one side only.

Note – Preprinted paper, e.g., with service logo, may generally be used but the imprint shall be outside the text of message field.

B.4 *Information fields*

The maximum size of each field corresponds to an area occupied by a given number of lines based on 6 lines/inch (4.23 mm/line) and a given number of characters based on 10 characters/inch (2.54 mm/character). Other forms of rendition and settings are possible.

These fields may be arranged on the pages according to national requirements. Figures B-2/F.415 and B-3/F.415 give two variations of the first page. Figure B-4/F.415 illustrates the layout of the second and following pages.

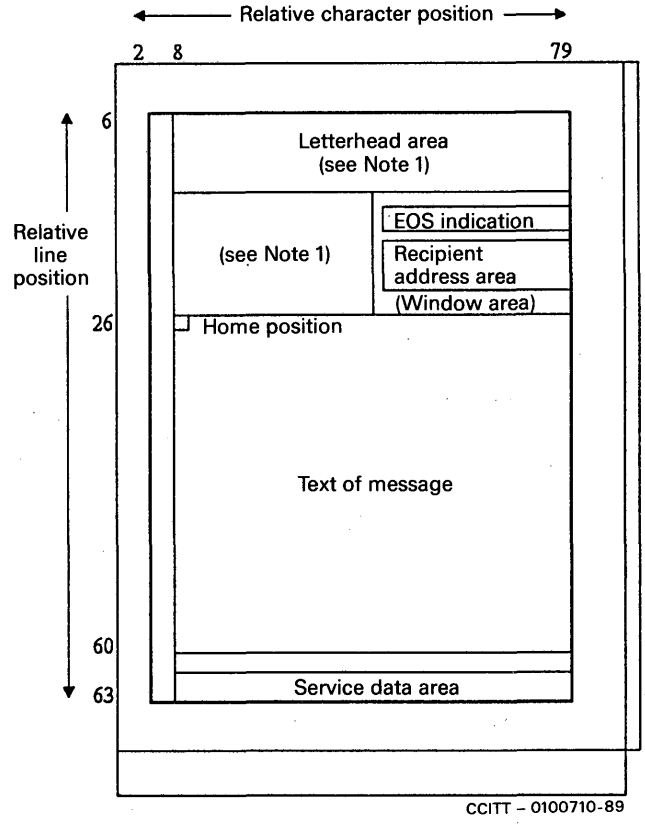


Note 1 - Area may be used for originator address.

Note 2 - For illustration purposes - not to scale. Relative positions based on 10 characters and 6 lines per inch.

FIGURE B-2/F.415

Illustration 1 of a first page



Note 1 - Area may be used for originator address.

Note 2 - For illustration purposes - not to scale. Relative positions based on 10 characters and 6 lines per inch.

FIGURE B-3/F.415

Illustration 2 of a first page

B.4.1 *Letter-head field*

The letter-head field is used to present the letter head as commonly used for business letters (with logo, originator address, references etc.). The use of the letter-head field is under the control of the PDAU and not of the user. The remaining space in the letter-head field can be used by the PDAU for other data, e.g., an MH address of the originator, which might be useful for replying through MHS.

The size of the letter-head field is limited to 6 lines of 72 characters each. The originator address (30 characters per-line) is one subfield in the letter-head field.

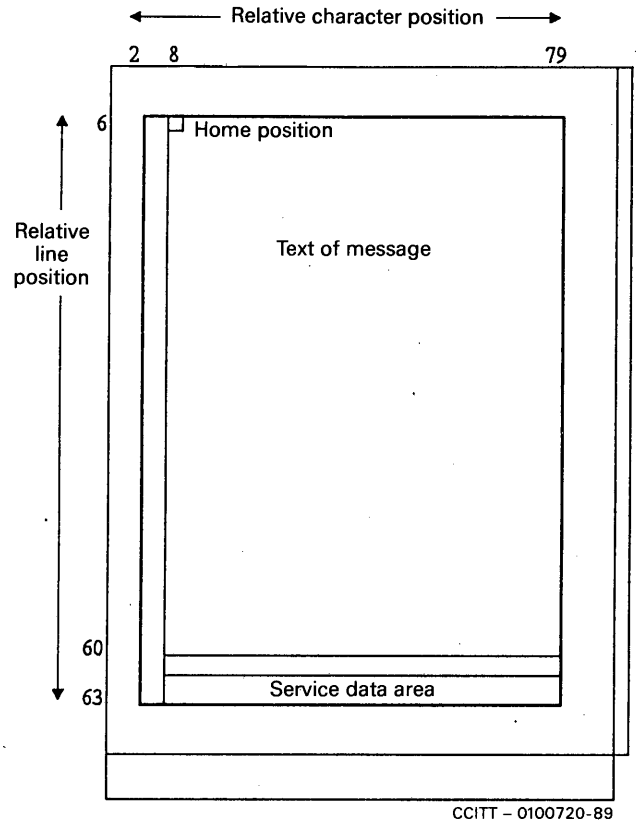
In the basic mode, only graphic characters which are generated by the MTA/PDAU from protocol data can be presented. The use of photographic elements and/or prestored logos and signatures is not part of the basic mode.

B.4.2 *Window area*

The window area is the area which is fully seen through the window of the envelopes considering also the play of the physical message in the envelope. This area contains all the information required for handling and delivery of the physical message by the PDS, and remains free of all other information (no wording or extraneous matter).

The window area may be either on the left or on the right depending on national practice.

Note – The use of double window envelopes is considered a national matter.



Note – For illustration purposes – not to scale. Relative positions based on 10 characters and 6 lines per inch.

FIGURE B-4/F.415

Illustration of second and following pages

B.4.2.1 *Elements of service indication field*

The elements of service indication field covers an area of 1 line comprising 30 characters. This area is to indicate all the options requested by the originator for the handling of the physical message (e.g., special delivery).

This handling may be indicated in descriptive terms or by the use of codes.

It may be necessary to give additional indication in a form commonly used in the PD service; for example, by affixing stickers on the envelope. This is a national matter.

B.4.2.2 *Space line field*

The space line field shall be free of imprinted information. The space line is essential to ensure that information above the address is to be clearly separated.

B.4.2.3 *Postal address field*

This postal address field contains the postal address of the recipient. It covers a field of 6 lines of 30 characters each.

B.4.3 *Text of message*

The text of message field is used to present the content of the message. In the case of IP-messages, this field is composed of the IPM heading and body.

The maximum size of this field is:

a) on the first page, 35 lines of (72 + 5) characters each and,

b) on the following pages, 55 lignes of (72 + 5) characters each.

Note 1 – The text of the message is presented relative to the home position. The home position is in the first line of the field text of message and approximately 20 mm from the left paper edge (position 8).

Note 2 – 72 characters may be presented from position 8 to position 79 and 5 characters to the left of position 8 (positions 3 to 7).

Note 3 – The utilization of the extra "+5" character spaces mentioned above requires the use of backspace.

B.4.4 *Service data field*

The service data field is used to present service data, e.g., time stamps, message identifier and page numbers. This field is recommended to extend over two lines of 72 characters each.

Note – The service data field may also cover more or less than 2 lines; this is considered a national matter.

B.5 *Control codes for inserting machines*

Printing in position 3 to 7 is only allowed in the text of message field. In other fields, this space is reserved for bar codes controlling the enveloping process where automated paper handling equipment is used. In these cases, the bar codes could be used on all pages of the physical message.

B.6 *Character sets*

The MTA/PDAU supports the use of the following encoded information types:

- Telex;
- IA5 text, (IRV);
- Teletex.

Support of additional encoded information types is for further study. Additional encoded information types may be used under bilateral agreements.

It is an objective of the MH/PD service intercommunication to make the most use of electronic printers to ensure that the whole basic set of graphic characters received are rendered without ambiguity or loss of information.

It is therefore preferred that each PDAU will at least provide for the rendition of the full basic set of graphic characters from Figure 2/T.61.

However, it may be unavoidable that messages have to be converted into a 7-bit set such as defined in Recommendation T.50 for further processing and rendition in some countries.

The selection of a print font is considered to be a national matter. Fonts which are commonly used in a country should be chosen. Rendition rules for the representation of the basic character set of Figure 2/T.61 are also a national matter.

B.7 *Code conversion*

Conversion from telex and IA5 (IRV) to T.61 for further processing and rendition in the MTA/PDAU follows the rules given in Annex A.

If conversion to a 7-bit encoded set in unavoidable, conversion from telex and IA5 (IRV) shall be according to Recommendation X.408. Conversion of messages received encoded in the T.61 set shall be converted in the greatest possible extent to minimize ambiguity and loss of information.

B.8 *Format conversion*

The constraints of format conversion for the content of the message are as given in § B.4.3.

These constraints define the presentation space of the X-and-Y directions as defined in Recommendation X.408.

Folding of the lines and pages to the constraints of the PDAU is considered a loss of information according to Recommendation X.408.

To recover from loss of information the PDAU may apply the following fallbacks:

- If the originator's line length is greater than 72 characters, but not more than 80 characters, the messages will be printed with 12 cpi instead of 10 cpi.
- If the originator's first page length is greater than 35 lines but not more than 55 lines, the message will be printed starting on the second page (see Note).
- In the case of IP-messages, the rendition of the IPM header is under the control of the PDAU. The user wil not know the remaining number of lines on the page on which the header is printed. Thus, if the first page of the body parts fits into the remaining space, it will be printed on that same page; otherwise it will be printed on the next page (see Note).

Note – Notification of the recipient that the message was started on the next page, for example by a note, is a national matter.

Messages which are not paginated, either because pagination was not possible in the originator's text or because the originator didn't use pagination, will be folded to pages by the PDAU.

ANNEX C

(to Recommendation F.415)

Undeliverable mail diagnostics

C.1 *Reasons related to the address*

- Physical delivery address incorrect (does not exist).
- Physical delivery office incorrect or invalid (does not exist).
- Physical delivery address incomplete.

C.2 *Reasons related to the recipient*

- Recipient unknown.
- Recipient deceased.
- Organization expired.
- Recipient refused to accept.
- Recipient did not claim.
- Recipient changed address permanently (moved), forwarding not applicable.
- Recipient changed address temporarily (on travel), forwarding not applicable.
- Recipient changed temporary address (departed), forwarding not applicable.

C.3 *Reasons of non-forwarding*

- New address unknown.
- Recipient did not want forwarding.
- Originator prohibited forwarding.

C.4 *Reasons related to the PDAU capabilities*

- Physical rendition not performed.
- Physical rendition attributes not supported.

APPENDIX I

(of Recommendation F.415)

Naming and addressing examples

I.1 *Example 1*

I.1.1 *Postal O/R address*

PD country name:	DE (Germany, Federal Republic of)	
Country Name:	DE (Germany, Federal Republic of)	
Administration domain name:	DBP (Deutsche Bundespost)	
PD service name:	POST	
Postal Code:	6000	
Version 1 (unformatted)	*Version 2 (formatted)*	
Franz Müller	Personal name:	Franz Müller
Rüdesheimer Str. 21	Street address:	Rüdesheimer Str. 21
6000 FRANKFURT 1	PD office name:	FRANKFURT
	PD office number:	1

I.1.2 *Rendition of Postal Address*

The following printout appears on the first page of the letter and is visible through the window of the envelope.

Franz Müller
Rüdesheimer Str. 21
6000 FRANKFURT 1 (see Note 1)
BUNDESREPUBLIK DEUTSCHLAND (see Note 2)

Note 1 – The postal code and country name will automatically be taken from the MHS routing data.

Note 2 – Country name is optional, except in the case of transit mail.

I.2 *Example 2*

I.2.1 *Postal O/R address*

PD country name:	CA (Canada)	
Country name:	CA (Canada)	
Administration domain name:	CPC (Canada Post Corporation)	
PD service name:	EMAIL	
Postal code:	K2E 7L9	
Version 1 (unformatted)	*Version 2 (formatted)*	
Mr. J. Doe	Personal name:	Mr. J. Doe
ACME Corp.	Organization name:	ACME Corp.
141 Anyname Avenue	Street address:	141 Anyname Avenue
SMALLTOWN, Ontario	PD office name:	SMALLTOWN, Ontario

I.2.2 *Rendition of postal address*

The following printout appears on the first page of the letter and is visible through the window of the envelope.

Mr. J. Doe
ACME Corp.
141 Anyname Avenue
SMALLTOWN, Ontario
K2E 7L9 (see Note)

Note – The postal code and country name will automatically be taken from the MHS routig data.

Recommendation F.420

MESSAGE HANDLING SERVICES: THE PUBLIC INTERPERSONAL MESSAGING SERVICE

The establishment in various countries of message handling services in association with public networks creates the need to produce Recommendations covering the aspects of public message handling services.

The CCITT,

considering

(a) the need for public message handling services;

(b) the strategic and commercial importance of standardization of message handling services;

(c) the urgent need for intercommunication agreements for existing telematic services, and other services with public message handling services;

(d) the need for a clear distinction between the responsibilities to be allocated to service providers and those of subscribers and/or users;

(e) the need for establishing international compatibility between different messaging systems;

(f) the growth of the installed base of terminals and personal computers with the ability to access message handling systems;

(g) that several F-series Recommendations describe public message handling services;

(h) that certain X and T-series Recommendations cover relevant aspects of systems used for the provision of messaging services,

unanimously declares

the view that the requirements specified in this Recommendation should be applied for the provision of the public interpersonal messaging service internationally.

CONTENTS

1 Purpose and scope

1.1 *General*

This Recommendation specifies the general, operational and quality of service aspects of the public international interpersonal messaging service. interpersonal messaging services provided by Administrations belong to the group of telematic services defined in the F-series Recommendations.

This type of message handling service is an international telecommunication service offered by Administrations, enabling subscribers to send a message to one or more recipients and to receive messages via telecommunication networks using a combination of store-and-forward, and store-and-retrieve techniques.

Locally provided functions, for which communication with other subscribers is not required, are not covered by CCITT Recommendations.

The Interpersonal Messaging (IPM) Service enables subscribers to request a variety of features to be performed during the handling and exchange of messages.

Some features are inherent in the basic IPM service. Other non-basic features may be selected by the subscriber, either on a per-message basis or for an agreed contractual period of time, if they are provided by Administrations.

Basic features have to be made available internationally by Administrations. Non-basic features, visible to the subscriber, are classified as either essential or additional. Essential optional features must be made available internationally by Administrations for national use and internationally on the basis of bilateral agreement. Non-basic features are called *optional user facilities.*

IPM service may be provided using any physical network. IPM service may be offered separately or in combination with various telematic or data communication services. It can be obtained by making appropriate arrangements.

Technical specifications and protocols, to be used in the IPM service are defined in the X.400-series Recommendations, in Recommendation T.330 and in Recommendation U.204.

This service definition is contained in § 2. Requirements for intercommunication between subscribers are described in §§ 3 and 4. Section 5 describes naming and addressing, while §§ 6, 7 and 8 describe the operation of the service, quality of service, tariff and accounting principles. Network requirements are given in § 9. The provision of subscriber information is in § 10, and § 11 contains information on the use of IPM service within CCITT defined telematic services.

1.2 *Message handling systems used in the provision of IPM service*

1.2.1 *1984 implementations*

This service Recommendation assumes that the message handling systems implemented to provide the service outlined herein are based on the 1988 version of the X.400-series Recommendations. It is recognized however that for some time after the publication of this Recommendation, the majority of implementations of IPM service will be based on the 1984 X.400-series of Recommendations. Administrations are encouraged to adopt the latest CCITT Recommendations; however, in the interim, they may make use of this Recommendation with 1984 implementations as outlined below.

1.2.2 *Elements of service*

Elements of service available for message handling services are listed and classified in Recommendation F.400. Annex C provides a list of all the elements of service (called service elements in 1984) for IPM from the 1984 X.400 Recommendation. In addition, the classification of each element of service as they were in 1984 in Recommendation X.401 are shown. In the 1988 X.400 Recommendation, there are many new elements of service representing the new functionality that were not present in 1984. Most of these have been classified as additional, meaning that they do not have to be supported, hence the 1984 implementations can make use of this service Recommendation in most cases. Other differences between 1988 and 1984 are of two types, new elements of service that are classified as essential, and old (meaning 1984) elements of service that have been re-classified as essential for 1988. Annex C of Recommendation F.400 lists both the new elements of service in 1988 as well as changes in classification to any 1984 elements of service. In both cases, to allow for 1984 implementations to be used for the provision of public IPM service as described in this Recommendation, a grace period of 8 years is provided for Administrations to upgrade their implementations in this respect to the 1988 technical Recommendations.

1.2.3 *Name forms*

The specification of the name forms in the 1988 Recommendations have been enhanced and postal O/R addresses have been added. The name forms and the mandatory components of the 1984 Recommendations have their equivalence in the new framework and are aligned in principle.

1.2.4 *Interworking*

In order to protect the investment of Administrations who have implemented 1984 systems for the provision of IPM service, 1988 ADMD implementations shall be able to interwork to 1984 ADMDs as outlined in Recommendation X.419, Annex B.

Interworking from 1988 ADMDs to 1984 PRMDs is a national matter.

2 IPM service

2.1 *General service requirements*

2.1.1 The fundamental ability of the IPM service is to provide a public interface between originators and recipients to enhance their means of communication especially where there is no immediate or convenient direct telecommunication service available between subscriber's equipment or the telecommunication services available are incompatible.

This service may also provide features available for the preparation and the presentation of the messages.

2.1.2 The IPM service will be provided by Administrations using the message transfer service defined in Recommendation F.410, and by systems that conform to the X.400-series of Recommendations.

Management domains (MDs) are defined for the purpose of responsibility boundaries. The MD managed by an Administration is called an administration management domain (ADMD). The MD managed by an organization is called a private management domain (PRMD).

2.1.3 International exchange of messages are performed between administration management domains through CCITT-standardized public data transmission services.

2.1.4 Different body part types of messages may be exchanged through this service. The urgent body part types are listed in § 3.

2.1.5 An Administration may provide subscribers with different methods of access to the IPM service. The possible methods are:

1) directly from the user's terminal;
2) via a private message handling system.

2.1.6 Each Administration is responsible for the national access to its management domain.

2.1.7 The characteristics of the interfaces and access methods used between terminals and the IPM service are a national matter, although they may follow various CCITT-standardized services such as telex, teletex, facsimile videotex or data transmission services. However, the IPM service optional user facilities offered are defined and are independent of the access method and user's terminal.

2.1.8 The national implementation of the IPM service may provide intercommunication with existing services such as telex, teletex, facsimile and videotex. When implemented, the interfaces between the IPM and the other services shall be according to relevant CCITT Recommendations.

2.1.9 As the service is providing indirect communication, cases of non-delivery of the message to the intended recipient may occur. The IPM service provides for non-delivery notification and, as optional user facilities, for delivery, receipt and non-receipt notifications.

2.1.10 Due to the intermediate storage of the message, the service may provide conversion optional user facilities: speed, access procedures, networks, and coding of message contents.

2.1.11 The message belongs to the originator until delivery has taken place. After delivery, the message belongs to the recipient.

2.1.12 Where a sender and recipient have different and conflicting requirements, the sender's requirements shall take precedence (e.g., body type conversion or redirection control).

2.2 *IPM service features*

2.2.1 *Introduction*

Recommendation F.400, § 19, defines elements of service which are available in the IPM service and are classified as either belonging to the basic service or as IPM optional user facilities. Elements of service comprising the basic IPM service are inherently part of the service and are always provided and available. The optional user facilities that are classified as essential are always provided and those classified as additional may be available nationally, or internationally on the basis of bilateral agreement.

2.2.2 *Basic IPM service*

A set of elements of service comprises the basic IPM service. This set is defined in Recommendation F.400, and listed in Table 10/F.400. The basic IPM service, which is built upon 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, which are a set of computer application processes, cooperate with each other to facilitate communication between their respective users. To send an IP-message, the originating user makes a request of his UA, specifying the name or address 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 followed by the recipient. To facilitate meaningful communication, a receiving user may specify the encoded information type(s) that can be contained in IP-messages delivered to him, as well as the maximum length of a message he is willing to have delivered to him. The original encoded information type(s) and an indication of any conversions that may have been performed and the resulting encoded information type(s) are supplied with each delivered IP-messages. In addition, the submission time, delivery time and other capabilities are supplied with each IP-message. Non-delivery notification is provided with the basic services.

2.2.3 *IPM optional user facilities*

A set of the elements of services of the IPM service are optional user facilities. The optional user facilities which may be selected on a per-message basis or for an agreed contractual period of time, are listed in Tables 11/F.400 and 12/F.400, respectively. Local user facilities may be usefully provided in conjunction with some of these user facilities.

The optional user facilities of the the IPM service that are selected on a per-message basis are classified for both origination and reception by UAs. If an Administration provides the IPM service and 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 Administration provides the IPM service and offers these optional user facilities for reception by UAs, then the receiving UA 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 or essential 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 service.

2.2.4 *Local functions*

The MHS may perform many local functions for its subscribers in addition to providing IPM features. For example, to assist subscribers in preparing and editing IP-messages, MHS may provide an editing capability. This editor could operate on a single line of text at a time, or it could permit the display and alteration of a page at a time. A subscriber may have to access MHS frequently to determine if new messages have arrived. Alternatively, the MHS could alert the subscriber when new messages have arrived (for example, by setting a message light on his telephone, or by his displaying on his desktop terminal the originator's name and subject of all unread messages or by computer-initiated voice indication).

The MHS may provide local database controls to help the subscriber find previously received and filed IP-messages (for example, to find the message from Mr. Jones delivered sometime in August on the subject of *teleconferencing*). A subscriber on vacation may request the MHS to automatically forward all his IP-messages to his delegate, or define rules for which IP-messages should not be auto-forwarded (for example, personal messages).

Local services such as those above, while perhaps utilizing some of the IPM features, do not require coordination or cooperation with other subscribers. Thus they do not impact the communication protocols associated with MHS. Therefore, local functions that may be provided by Administrations are outside the scope of CCITT.

2.3 *Responsibility boundaries*

The purpose of the MHS is to allow messages to be submitted for transfer to the destination and to be delivered to a UA/MS whose address is specified by the originator.

A user interacts with his UA on the sending and on the receiving side. On his request, a message is submitted to the MTS. He is also able to retrieve a received message from his UA or MS.

The responsibility for the message rests in the MHS when the originating user gives the command to send the message. The responsibility for a message is turned over to the receiving UA/MS after successful delivery. If the UA or MS is provided by an Administration, the responsibility for the message is taken over by the user when he reads the message.

As a basic feature, a non-delivery notification is created by the MHS when delivery to the receiving UA/MS is not possible. The conditions applied to this criteria may also depend on optional user facilities, e.g. conversion prohibition. An originating user may, for a particular message, specifically request a delivery notification, and/or a receipt notification, and/or a non-receipt notification.

In the case of telematic addresses or telex addresses, delivery takes place automatically when the message is transmitted to the receiving terminal. The responsibility of the MHS ends when the message is received by the terminal. After delivery to a document store, or a message store, responsibility turns over to the user after having read the message once. When leaving the message in the store, the responsibility will be defined by the service provider.

Loss of information may occur through the process of conversion as long as the conversion is not explicitly prohibited by the originating user.

The responsibility of messages transferred through MDs starts at the moment of entering the domain and ends when leaving the domain; however, a later audit must be possible.

When an ADMD interacts with a PRMD, 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 MT service, the ADMD is responsible for ensuring that the accounting, logging, quality of service and other related operations of the PRMD are correctly performed. An ADMD acts as the naming authority for the associated PRMDs.

2.4 *Message store*

Administrations may optionally provide message store (MS) to permit delivery of messages so that the recipient's UA does not have to be on line continuously. This is described in Recommendation F.400, § 7.4. A message delivered to an MS is deemed delivered by MHS. Messages delivered to an MS can be retrieved by the recipient at his convenience and various optional user facilities can be provided to allow for retrieval for listing, fetching, and deletion of messages. When subscribing to an MS, all messages destined to the UA are delivered to the MS, and if the UA is on line, an alert will be sent to the UA (from the MS) to inform the user of the fact that a message just arrived.

2.5 *Use of directory*

By making use of directory systems, IPM users will be able to address recipients by using directory names or distribution list names, which are more user friendly than O/R addresses. The MHS will be able to access a directory system and find out the O/R address(es) corresponding to a given directory name or distribution list name, for delivery of a message. This capability is described in Recommendation F.400, § 14.

2.6 *Security*

Administrations may optionally provide security mechanisms as outlined in Recommendation F.400, § 15, to counter the various security threats mentioned. This capability relies on a Directory System storing certified copies of public keys for MHS users.

2.7 *Distribution lists*

A group whose membership is stored in the directory can be used as a distribution list (DL). The originator simply supplies the name of the list on submission of a message, and the MHS can obtain the directory names (and then the O/R addresses) of the individual recipients, by consulting the directory. Upon receipt of a message addressed to a distribution list, the recipient can determine through which DL the message arrived. An originator can prohibit the expansion of the distribution if one of the recipients specified refers to a distribution list. Recommendation F.400, § 14, outlines the full capabilities available to DL users.

If a user unknowingly sends a message to a DL, he may incur charges for multiple deliveries that he was not expecting. Because of this, names of distribution lists should be indicative of the fact that what is being named is a DL. Owners of DLs should also insure that they respect a potential member's wishes about being a member and the rules of the country of the member that may prohibit inclusion without prior agreement.

2.8 *Intercommunication with physical delivery services*

The intercommunication with the physical delivery services is an optional capability of the IPM service that allows for the sending of a message from an IPM user to a recipient via physical means, such as the traditional postal service. To invoke the capability, the originating user shall use the requested delivery method element of service on submission of his message, specifying physical delivery. The message may be addressed using the postal O/R address, or the directory name of the intended recipient, in which case the MHS will consult the directory system to determine the postal O/R address, The use of MH/PD service intercommunication by IPM users is described in Recommendation F.415 and Recommendation F.400, § 10.

3 Types of body parts

Messages sent and received in the IPM service can be composed of one or more body parts. Applicable body part types are defined in Recommendation X.420 and comprise the following:

- IA5 text,
- Voice,
- G3 facsimile,
- G4 class 1,
- Teletex,
- Videotex,
- Encrypted,
- Message (e.g., for a forwarded message),
- Mixed mode,
- Bilaterally defined,
- Nationally defined,
- Externally defined.

4 Conversion between different encoded information types

The MTS provides conversion functions to allow IPM users to input messages in one encoded format, called encoded information type (EIT), and have them delivered in another EIT to cater to users with different terminal types. This capability is inherent in the IPM service, and increases the possibility of delivery by tailoring the message to the recipient's terminal capabilities. The EITs supported for the IPM service are defined in Recommendation X.420. IPM users have some control over the conversion process through various elements of service as described Recommendation F.400/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, and 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. The definition of loss of information is given in Recommendation X.408.

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 EIT was.

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

5 Naming and addressing in general

In 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 nad DLs are identified by O/R names. O/R names are comprised of directory names and/or O/R addresses, all of which are described in this section. Recommendation F.401 provides more detail on naming and addressing for public message handling services, including naming restrictions and responsibilities of Administrations.

5.1 *Directory names*

Users of MHS service, and DLs, may be identified by a name, called a directory name. A directory name has to be looked up in a directory to find out the corresponding O/R address. The structure and components of directory names is described in the X.500 series of Recommendations.

A user may 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 may use the directory name and have the MHS access the directory to resolve the corresponding O/R address or addresses automatically.

Every MHS 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.

5.2 *O/R names*

Every MHS user or DL will have an O/R name. An O/R name comprises a directory name, an O/R address, or both. The directory name unambiguously identifies an MHS user but not necessarily uniquely. The O/R addres uniquely identifies an MHS user.

Either or both components of an O/R name may be used on submission of a message. If only the directory name is present, the 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 the directory name is absent, it will use the O/R address, but will carry the directory name and present both to the recipient. If the O/R address is incorrect, it will then attempt to use the directory name as above.

5.2 *O/R addresses*

An O/R address contains information that enables the 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).

Various forms of O/R addresses are currently defined, each serving its 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 with numeric keypads.
- *Postal O/R address:* Provides a means of identifying originators and recipients of messages and notifications, for physical delivery.

An O/R address is made up of a collection of information called attributes. These attributes as used in each of the O/R address forms above are detailed in Recommendation F.401.

Management domains shall allow their users to originate messages using any of the above forms. The form in which names are input by or presented to the subscriber is a national matter (as for example the use of distribution lists or of friendly ways of identifying user agents).

Each Administration is responsible for the unique identification of each user agent in its management domain.

6 Operation of the service

6.1 *General*

6.1.1 The IPM service provides that messages can be sent, transferred, delivered and received, using fully automatic procedures.

Note – Manual receipt and sending of message can be provided in the case of interworking with postal systems.

6.1.2 Messages are prepared in, sent from, and delivered to a memory. These memories are part of the User Agent/MS functionality and are under control of the subscriber.

6.1.3 The transfer of messages between management domains will be in accordance to the message transfer service as described in CCITT Recommendation F.410.

6.1.4 Each Administration providing the IPM service should validate the subscribers' identities, at the time of access.

Note – Further study is needed in the case of auto-receipt.

6.1.5 It is a national matter whether to allow private messaging systems to connect to the public IPM service, in order to allow users of these systems to exchange messages. If these interconnections are provided, they should take place between Administration management domains in accordance with CCITT Recommendations.

6.1.6 When implicit conversion is provided by the Adminstration via the message transfer service, the message vill be converted if necessary, unless prohibited by the originator. The conversion will be in accordance to the rules specified in CCITT Recommendations X.408. See also § 4 of this Recommendation.

6.1.7 Deferred Delivery shall be provided by the management domain of the originator, which is responsible for the storage of the message until the date and time specified for intended delivery. Therefore the element of service, deferred delivery, should not be used across international links.

6.2 *Message handling phases*

6.2.1 *General*

The IPM service has different message handling phases visible to the user.

6.2.2 *Preparation phase*

In this phase, messages are prepared by making use of the User Agent functionality (e.g. editing and filing). The way in which these functions are performed is outside the scope of this Recommendation.

6.2.3 *Sending phase*

In this phase, the originator may request the user agent or message store to send a prepared message to one or more recipients and to request certain optional user facilities.

6.2.4 *Receipt phase*

In this phase, the subscriber can receive delivered messages and notifications from his user agent or message store. The receipt phase can be initiated by the service (auto-receipt) or by the subscriber for message reception. The operation of the user agent receiving messages is specified in Recommendation X.420.

Subscribers using terminals without user agent functionality may registter for a contractual period of time during which they will receive delivered messages automatically from their user agent to a terminal, if the Administration provides for this alternative. Normally the user agent is called to receive incoming messages.

In the case of auto-receipt, the MHS will initiate a call to the subscriber's terminal. In the other case, the subscriber shall initiate a call to the MHS at a time convenient to the subscriber.

The body parts of the message will be received by the subscriber in the form in which the originator has sent it, unless conversion has been performed.

For messages delivered to a teletex access unit, Recommendation T.330 defines the optional means by which the subscriber may receive or retrieve delivered messages.

The indication of the optional user facilities requested by the originator are presented by the user agent to the recipient in a form convenient to him.

Notifications: Four notifications can be received:

- non-delivery notification;
- delivery notification;
- receipt notification;
- non-receipt notification.

Non-delivery notification is automatically originated by the MTS, while delivery notification, receipt and non-receipt notification depend on the action of the recipient. In the case of a message to a teletex terminal, (auto) receipt notification may be returned by the TTXAU.

7 Quality of service

7.1 *Message status*

The unique identification of each IP-message enables the system to provide information about, e.g., the status of an IP-message.

In the event of system failure, all accepted and non-delivered messages should be traceable. If messages cannot be delivered, the originator must be informed by a non-delivery notification.

7.2 *Support by Administrations*

Administrations should provide assistance to their subscribers, with regard to non-delivery notifications not being received in due time, as far as public system components are concerned. Additional provision on support of status and tracing of messages may be provided under national responsibility.

When the user agent is provided by an Administration, additional functionality should be provided in order to minimize cases of not reading messages within a certain period of time (the definition of this period is for further study). This functionality could be, for example, alert messages sent to an automatic reception terminal.

7.3 *Model of delivery and notification times* (see Figure 1/F.420)

7.4 *Message delivery time targets*

The management domain of the recipient UA should force non-delivery notification if the message has not been delivered before x hours after submission (or after date and time indicated for deferred delivery), the value of x being dependent on the grade of delivery requested by the originator. (See Recommendation F.410, § 4.4.)

7.5 *Delivery notification time targets*

Non-delivery notifications or requested delivery notifications should be returned on a per-recipient basis, in order not to delay notifications for those messages in a multi-addressed message which have already been delivered, to enable the originating management domain either to return per-recipient notifications or to batch notifications to its subscribers. (See Recommendation F.410, § 4.5.)

7.6 *Receipt notifications and non-receipt notifications*

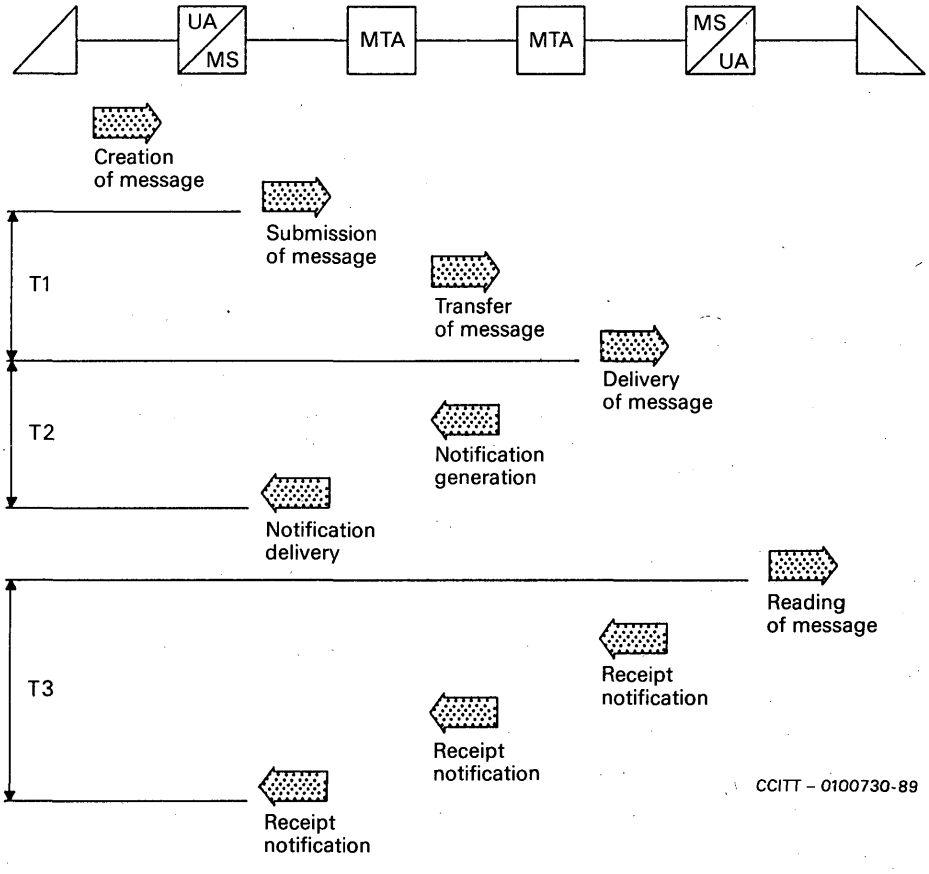
Delivery times for receipt or non-receipt notifications in the first place depend on local arrangements. When they are initiated by the receiving UA/user, they have the same time targets as the messages that cause them to occur (see Table 1/F.420).

7.7 *Error protection*

Error protection on transmission is provided by the MHS and underlying protocols used in the provision of the IPM service.

7.8 *Availability of service*

In principle, the IPM service should be available continuously. The user agent should be available for submission of delivery continuously (unless hold for delivery is invoked). In cases where the UA is not available for delivery continuously, a message store should be used.



T1 Delivery time
T2 Delivery notification time } For more details, see Recommendation F.410.

T3 Receipt notification time

Note 1 – Starting time of T3 corresponds to the time the message is displayed to the user and Receipt Notification is actioned by the user.
Note 2 – Ending time of T3 is the time that the Receipt Notification is made available to the user through the UA or MS.
Note 3 – Similar considerations apply to Non-receipt Notifications.

FIGURE 1/F.420

Notification time model

TABLE 1/F.420

Grade of delivery (of the referred message)	95% delivered before
Urgent	0.75 hours
Normal	4 hours
Non-urgent	24 hours

Note – Intercommunication with PRMDs is not included in the calculation of the time targets.

7.9 *Minimum storage capacity*

The storage capacity of a user agent and message store shall be sufficient to provide a high grade of service.

Note – This is for further study.

8 Tariff and accounting principles

See D-series Recommendations.

9 Network requirements

The IPM service is network independent, that is, the basic service and the essential optional user facilities are provided independently of the type of network used for service access. Additional optional user facilities chosen by an Administration to offer may vary.

10 User information and support

A directory shall be provided by each Administration for its domain. The directory can be hard copy or preferably electronic form.

The directory shall at least contain the following:

a) how to use the directory and the service;

b) list of O/R addresses of subscribers belonging to the Administration's domain;

c) list of standardized abbreviations for O/R address attributes;

d) list of country and Administration management domain names reachable by the public IPM service.

11 Use of the IPM service within CCITT-defined telematic services

See relevant F-series Recommendations.

ANNEX A

(to Recommendation F.420)

Abbreviations

The following abbreviations are used in this Recommendation.

A	Additional Optional User Facility
ADMD	Administration Management Domain
DL	Distribution List
E	Essential Optional User Facility
EIT	Encoded Information Type
G3	Group 3 (Facsimile)
G4	Group 4 (Facsimile)
IA5	International Alphabet 5
IP	Interpersonal
IPM	Interpersonal Messaging
MD	Management Domain
MHS	Message Handling System
MS	Message Store
MT	Message Transfer
MTA	Message Transfer Agent
MTS	Message Tranfer System
N/A	Not Applicable
O/R	Originator/Recipient
PD	Physical Delivery
PDN	Public Data Network
PDS	Physical Delivery System
PRMS	Private Management Domain
TTXAU	Teletex Access Unit
UA	User Agent

Note 1 – For a glossary of terms see Annex A to Recommendation F.400.

Note 2 – For references see Recommendations F.400 and F.401.

ANNEX B

(to Recommendation F.420)

Subscriber access and terminal requirements

B.1 *General*

Various types of terminals may be used for accessing the service. These terminals are functionally divided into two categories: those without user agent functionality, and those with user agent functionality. The telematic terminals assume a special user agent. Telex terminals belong to that first category.

B.2 *Terminals without UA functionality*

Terminals in this category require additional functions to be provided by MHS to enable their participation in the IPM service.

B.2.1 *Telex terminals*

Telex terminals shall conform to the relevant technical Recommendations, and be based on the relevant service Recommendations.

B.2.2 *Teletex terminals*

Teletex terminals shall conform to Recommendations T.60 and T.61. Documents which are exchanged between teletex terminals and the IPM service shall be in conformance to Recommendation F.200.

The access procedures for submission and delivery of documents shall conform to Recommendation T.330.

Note – The use of the interactive session protocol for submission and delivery is for further study. The ability to provide IPM service for documents using teletex standardized options is for further study.

B.2.3 *Facsimile terminals*

Group 3 and Group 4 facsimile terminals should have access to the IPM service.

Note – Access procedures are for further study.

B.2.4 *Videotex terminals*

These terminals shall conform to Recommendation F.300.

Note – Access procedures are for further study. Eventual subset of Recommendation F.300 needs to be considered.

B.2.5 *IA5 terminals*

The IA5 terminals are terminals able to send and receive messages encoded by characters chosen from the International Alphabet No. 5 (Recommendation T.50). The access procedures shall be based on one of the applicable procedures specified in Recommendations X.20 to X.32. These procedures describe the possibility for access to PDNs for data transmission.

Note – Additional procedures are for further study.

B.3 *Terminals with UA functionality*

These terminals shall, as a minimum, have the capabilities to:

1) provide the capabilities to subscribers of the basic features defined in § 2;
2) make use of the IPM protocol specified in Recommendation X.420;
3) use the submission and delivery protocol specified in Recommendation X.419;
4) use the remote operation procedures specified in Recommendation X.419.

These terminals shall be able to handle at least one EIT as defined in Recommendation X.408 (e.g., IA5, teletex, etc.).

ANNEX C

(to Recommendation F.420)

IPM service elements from 1984 X.400 Recommendations

Element of service	Classification			
	Basic	Optional		
		Origination	Reception	Contractual
Access management	X			
Alternate recipient allowed		A	A	
Alternate recipient assignment				A
Authorizing users indication		A	E	
Auto-fowarded indication		A	E	
Blind copy recipient indication		A	E	
Body part encryption indication		A	E	
Content type indication	X			
Conversion prohibition		E	E	
Converted indication	X			
Cross referencing indication		A	E	
Deferred delivery		E	N/A	
Deferred delivery cancellation		A	N/A	
Delivery notification		E	N/A	
Delivery time stamp indication	X			
Disclosure of other recipients		A	E	
Expiry date indication		A	E	
Explicit conversion		A	N/A	
Fowarded IP-message indication		A	E	
Grade of delivery selection		E	E	
Hold for delivery				A
Implicit conversion				A
Importance indication		A	E	
IP-message identification	X			
Message identification	X			
Multi-destination delivery		E	N/A	
Multi-part body		A	E	
Non-delivery notification	X			
Non-receipt notification		A	A	
Obsoleting indication		A	E	
Original encoded information types indication	X			
Originator indication		E	E	
Prevention of non-delivery notification		A	N/A	
Primary and copy recipients indication		E	E	
Probe		A	N/A	
Receipt notification		A	A	
Registered encoded information types	X			
Reply request indication		A	E	
Replying IP-message indication		E	E	
Return of contents		A	N/A	
Sensitivity indication		A	E	
Subject indication		E	E	
Submission time stamp indication	X			
Typed body	X			

Recommendation F.421 [1]

MESSAGE HANDLING SERVICES: INTERCOMMUNICATION BETWEEN THE IPM SERVICE AND THE TELEX SERVICE

The establishment in various countries of message handling service in association with public networks creates the need to produce Recommendations covering the aspects of public message handling services.

The CCITT,

considering

(a) the need for public message handling services;

(b) the strategic and commercial importance of standardization of message handling services;

(c) the urgent need for intercommunication arrangements for existing telematic services, and other services with public message handling services;

(d) the need for a clear distinction between the responsibilities to be allocated to service providers and those of subscribers and/or users;

(e) the need for establishing international compatibility between different messaging systems;

(f) the growth of the installed base of terminals and personal computers with the ability to access message handling systems;

(g) that several F-series Recommendations describe public message handling services;

(h) that certain X, T and U-series Recommendations cover relevant aspects of systems used for the provision of messaging services;

(i) that Recommendations F.60 and F.69 define the service requirements for the telex service;

(j) that Recommendation F.72 defines international telex store-and-forward;

(k) that the U-series Recommendations define the technical requirements for the telex service;

(l) that Recommendation U.204 defines the technical requirements for the intercommunication between the IPM service and the telex service;

unanimously declares

that operational procedures for intercommunication between the public interpersonal messaging service and the telex service shall be in accordance with this Recommendation.

CONTENTS

[1] This Recommendation is the same as Recommendation F.75 of which only the title appears in Fascicle II.4.

1 Scope

1.1 This Recommendation describes the general, operational and service procedures for the provision of intercommunication between the public interpersonal messaging service and the telex service.

1.2 The intercommunication is based on store-and-forward principles which allow users of one service to exchange messages with the users of the other service.

2 Introduction

The IPM service is a messaging service which may be provided on a variety of networks and allows several forms of addresses, whereas the telex service provides direct connection between subscribers in the telex network.

Therefore, to match dissimilar characteristics of the two services, it is necessary to provide intercommunication via a public telex access unit (PTLXAU). In both IPM service to telex service, and telex service to IPM service directions, the complete message is deposited in the PTLXAU for onward transmission.

In general the selection procedures for the telex subscriber will be two-stage; however, where the destination IPM service user is assigned a numeric address that is part of the national telex numbering plan of the destination country, one-stage selection procedures may be used.

3 Service outline

3.1 Communication between subscribers of the telex service and the IPM service is on store-and-forward basis; thus conversational mode interworking between users is not applicable.

3.2 Public access to the IPM service for telex subscribers and delivery of messages to telex subscribers from IPM service users is provided by means of a PTLXAU.

3.3 The PTLXAU belongs to the IPM service.

3.4 In the IPM service to telex service direction, the IPM service retains the responsibility for the message until delivery to the telex subscriber has been completed.

3.5 In the telex service to IPM service direction, the IPM service is responsible for the delivery of the message to the IPM service user, once the input is completed under normal conditions.

3.6 In both IPM service to telex service direction and telex service to IPM service direction, the international connection should be via the international telex network, as shown in Figure 1/F.421.

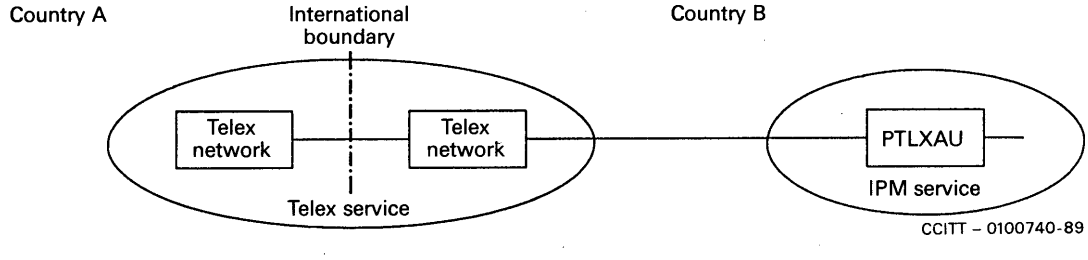


FIGURE 1/F.421

Model for service intercommunication

3.7 Where two Administrations offer an IPM service, the international boundary may be placed within the IPM service by bilateral agreement. In this configuration, however, international telex connections should continue to be established via the international telex network.

4 Operational procedures

4.1 *IPM service to telex service direction*

4.1.1 Messages from an IPM service user to a telex subscriber are sent as normal IP-message with the appropriate IPM elements of service, in accordance with Recommendation F.420.

4.1.2 When a message is received by the PTLXAU, the message content will be converted into the format and character repertoire defined for the telex service. This may result in loss of information if the IPM service user does not conform to these defined rules.

Note – The conversion process may take place in the message transfer system (MTS) associated with the PTLXAU.

4.1.3 The PTLXAU shall be responsible for the action to be taken for IPM elements of service received in accordance with Recommendation F.420. Annex B shows examples of IPM elements of service together with proposed actions to be taken by the PTLXAU.

4.1.4 Call establishment by and delivery of the message to the telex subscriber should be in accordance with Recommendations F.72 and U.204.

4.1.5 The IP-message sent to the called telex subscriber shall be preceded by a PTLXAU identification. The content of this identification is a national matter but should include the service code "CI", the code expression "IPM", and the telex network identification code in accordance with Recommendation F.69, e.g. "CI → IPM → CH".

4.1.6 A general layout of an IP-message delivered to the telex service is shown in Annex C.

4.1.7 The elements of service related to the IP-message heading shall be converted into printable text. The language of this text is a national matter. The PTLXAU shall transmit the originator O/R address to the called telex subscriber in the form necessary for recall, in accordance with the indications of Table 2/F.421 (see example in Annex C).

4.1.8 In order to help the telex recipients to recall the originator, the PTLXAU could transmit, as the first element of the message heading, some information as guidance. The contents of this field is a national matter, but when used should be called "FOR RECALL" (see Annex C).

4.1.9 Upon delivery of the message to the telex subscriber, a delivery notification should be sent back to the originating IPM service user if requested. In the event of non-delivery of the message to the telex subscriber, a non-delivery notification shall be sent back to the IPM service user (unless the IPM user has requested prevention of non-delivery notification).

4.2 *Telex service to IPM service direction*

In this direction, Administrations may implement either or both one-stage and two-stage call set-up procedures.

4.2.1 *One-stage selection*

4.2.1.1 Where one-stage call set-up procedures are used, the number assigned to a user in the IPM service must appear to be part of the national telex numbering plan.

4.2.1.2 The length of the number assigned to the IPM service user shall be in accordance with the relevant U-series signalling Recommendations.

4.2.1.3 The procedures for message transfer within the IPM service, e.g. mapping of the assigned number to an O/R address, are a national matter and not covered by this Recommendation.

4.2.1.4 The call shall be established using normal telex call set-up procedures.

4.2.1.5 The telex number received by the PTLXAU from the telex network shall be verified by the IPM service as being proper to a registered IPM service user. If the verification fails:

a) where the PTLXAU is provided by the Administration which also provides all or part of the telex network, the service signal NP may be returned;

b) where the PTLXAU is not provided by the Administration which also provides all or part of the telex network, the procedures to be applied shall be in accordance with Recommendation F.74.

4.2.1.6 The answerback returned to the calling telex subscriber at call establishment and also during the text input stage shall contain the national telex number assigned to the IPM service user.

4.2.1.7 The call shall be cleared using normal telex call clearing procedures.

4.2.1.8 When the message cannot be delivered to the IPM service user, a non-delivery notification shall be returned to the telex subscriber. The procedures for establishing the calling telex address are specified in Recommendation U.204.

4.2.1.9 The non-delivery notification returned to the originating telex subscriber should contain a reference consisting of the telex address of the IPM service user and time and date of submission to the PTLXAU.

4.2.1.10 The action to be taken when a non-delivery notification cannot be returned to the calling telex subscriber is for further study.

4.2.1.11 The format of notifications and the procedures for their delivery should be in accordance with Recommendation U.204.

4.2.1.12 The use of IPM elements of service by the telex subscriber is for further study.

4.2.2 *Two-stage selection*

4.2.2.1 The telex subscribers shall use normal telex call procedures to access the PTLXAU which is allocated a telex number that is part of the national telex numbering plan of the country in which the PTLXAU is located.

4.2.2.2 Procedures for access to the PTLXAU shall follow Recommendation U.204.

4.2.2.3 A service identifier may be input before the O/R address(es) of the first message. If may allow the Administrations to provide intercommunication with several services through only one PTLXAU (see Tables 1/F.421, 3/F.421 and Annex D).

4.2.2.4 The PTLXAU shall be able to accommodate the following O/R address forms:

- Mnemonic O/R address;
- Terminal O/R address;
- Numeric O/R address;

as specified in Recommendation F.401. The O/R address should be input in accordance with the requirements of Recommendation U.204.

It is the responsibility of the originating telex subscriber to be aware of the required attributes specific to the domain of the called IPM service user. Each attribute of the O/R address shall be identified and delimited. The complete O/R address shall be terminated with an end-of-address (EOA) indicator.

The structure of the service identifier and the address input is shown in Table 1/F.421.

Each attribute of the address structure shall be contained in one line.

Each address attribute and the service shall be identified by a code expression according to Tables 2/F.421 and 3/F.421.

4.2.2.5 Under normal conditions, the message input will be terminated by an end of message (EOM) or and end of transmission (EOT) signal. In case where no EOM or EOT signal is received, the PTLXAU shall forward any input received prior to call disconnect with the added text "THIS MESSAGE MAY BE INCOMPLETE". Annex D shows a general layout applicable in case of submission of message(s) to the PTLXAU by the telex subscriber.

4.2.2.6 Except as defined in 4.2.2.5 above, the action to be taken when abnormal conditions are encountered during message input shall be in accordance with Recommendation U.204.

TABLE 1/F.421

Telex service to IPM service address structure

Service identifier
Address attribute identifier <value>
.
.
.
Address attribute identifier <value>
End of single O/R address (+)
[Next O/R address(es)]
[Request for IPM elements of service]
End of address(es) (BT)
[Request for delivery notification]

Note – [ ] indicates optional attributes.

TABLE 2/F.421

Code expressions for address attribute identifiers

Address attribute	Format
Country name	CTN ⟶ <value>
Administration domain name	ADM ⟶ <value>
Private domain name	PRI ⟶ <value>
Organization name	ORG ⟶ <value>
Organization unit name(s)	OUN ⟶ <value>
Personal name	
– Surname	SUR ⟶ <value>
– Given name	GIV ⟶ <value>
– Initials	INI ⟶ <value>
– Generation qualifier	GEN ⟶ <value>
– Common name	COM ⟶ <value>
Numeric user identifier	NUS ⟶ <value>
Terminal type and network address	
for telex	TLX ⟶ <value>
teletex	TTX ⟶ <value>
facsimile	FAX ⟶ <value>
videotex	VTX ⟶ <value>
Domain defined attribute(s)	
– Type	DDT ⟶ <value>
– Value	DDV ⟶ <value>

Note 1 – The symbol ⟶ equals a space.

Note 2 – Allowed attribute values are specified in Recommendation F.401.

TABLE 3/F.421

Code expression for the service identifier

Service	Format
Interpersonal messaging service	IPM

4.2.2.7 During the input stage of the address, the PTLXAU shall validate, as a minimum, the following O/R address formats, as specified by the domain:

- The existence of mandatory attributes.
- The existence of non-allowed attributes.
- The minimum and maximum allowed number of characters in each attribute.
- The existence of non-allowed characters in an attribute.

Where applicable, the existence/non-existence of non-significant character(s) preceding or following the attribute values shall not prevent validation.

Despite the acceptance by the PTLXAU of the submitted O/R address, there is no guarantee that the message will be subsequently delivered and, in this case, the originating telex subscriber will be charged for a message which was not delivered. It is therefore desirable that a means of verifying the existence of the O/R address be provided and the method of achieving this is left for further study.

4.2.2.8 The service principles for delivery and non-delivery notifications should be in accordance with Recommendation F.72. The format of the notification messages is defined in Recommendation U.204. Delivery notification may be requested as a code expression following the end of address signal.

4.3 *Construction of the IP-message*

The message received by the PTLXAU shall be delivered to the IPM user(s) in accordance with following rules.

4.3.1 *P2 body part*

The received message, excluding the recipient address(es), shall form the body of the IP-message. All the received characters shall be delivered except the WRU signals.

4.3.2 *Recipient O/R address*

All recognized O/R addresses shall be assumed as primary recipients. By default, these primary recipients will not be disclosed to each other.

4.3.3 *Originator indication*

The calling telex subscriber address shall be converted by the PTLXAU into the format of a terminal O/R address and shall be placed in the originator indication element of service field.

4.3.4 *Subject indication*

The PTLXAU shall generate the element of service which will cause TELEX to appear in the subject indication element of service field.

4.3.5 *IP-message identification*

The content of the message reference information returned to the calling telex subscriber shall also be used as the unique identifier in the IP-message identification element of service field.

4.3.6 *Grade of delivery selection*

The PTLXAU shall set the grade of delivery selection element of service to the value URGENT.

4.3.7 *Conversion prohibition in case of loss of information*

The use of the element of service – conversion prohibition in case of loss of information – is for further study.

4.3.8 *Disclosure of other recipients*

This element of service shall be set by the PTLXAU when the originating telex subscriber requests the disclosure of other recipients. The procedures for requesting this disclosure are defined in Recommendation U.204.

4.3.9 *Deferred delivery*

This element of service shall be set by the PTLXAU when the originating telex subscriber requests deferred delivery of his message. The procedures for requesting deferred delivery are defined in Recommendation U.204.

Note – The code expressions to be used for the selection of the elements of service described in §§ 4.3.8 and 4.3.9 by the telex subscriber, are shown in Table 4/F.421.

TABLE 4/F.421

Code expressions for the use of IPM elements of service

IPM element of service	Format
Disclosure of other recipients	DUR
Deferred delivery	DEF ⟶ <value>
Delivery notification	BT, ACK [a]

[a] The request for delivery notification may be given together with the code for end of address(es) (BT) if delivery notification is required.

Note – The symbol ⟶ equals a space.

4.3.10 *Other elements of service*

Elements of service of the basic IPM service other than those specified above shall be set by the PTLXAU in accordance with the requirements of the domain to which it belongs.

ANNEX A

(to Recommendation F.421)

Abbreviations

A/B	Answerback
ACK	Request for Delivery Notification Signal
ADM	Administration Management Domain
BT	End of Address(es) Signal
CI	Conversation Impossible
COM	Common Name
CTN	Country Name
DDT	Domain Defined Attribute Type
DDV	Domain Defined Attribute Value
DEF	Deferred Delivery
DUR	Disclosure of other Recipients
EOA	End of Address
EOM	End of Message
EOT	End of Transacton
FAX	Facsimile
GEN	Generation Qualifier
GIV	Given Name
I	Initials
IP	Interpersonal
IPM	Interpersonal Messaging
MT	Message Transfer
MTS	Message Transfer System
NP	The called party is not, or no longer, a subscriber
NUS	Numeric User Identifier
O/R	Originator/Recipient
ORG	Organization Name
OUN	Organization Unit Name(s)
P2	IPM Protocol
PRI	Private Domain Name
PTLXAU	Public Telex Access Unit
SUR	Surname
TID	Terminal Identifier
TLX	Telex
TTX	Teletex
UTC	Universal Coordinated Time
VTX	Videotex
WRU	Who Are You
+	End of Single O/R Address signal
⟶	Space

Note 1 – For a glossary of terms see Annex A to Recommendation F.400.

Note 2 – For references see Recommendation F.400.

ANNEX B

(to Recommendation F.421)

Actions to be taken by the PTLXAU/examples

Basic IPM elements of service and essential optional IPM user facilities which have to be processed by the PTLXAU in the case where a message is sent from the IPM service to the telex service direction (Table B-1/F.421).

TABLE B-1/F.421

Reference Rec. F.400 Annex B	Elements of service	Action to be taken	Examples
B.5	Authorizing users indication	Display in message heading	Authority: ⟶ <value>
B.6	Auto-forwarded indication	Ignore	
B.8	Blind copy recipient indication	Display the O/R descriptor information of the blind copy recipient(s)	BCC ⟶ <value>
B.9	Body part encryption indication	The PTLXAU shall send a non-delivery notification to the originator	
B.12	Content type indication	National matter for content types different than P2	
B.13	Conversion prohibition	If ITA2, ignore. Otherwise the PTLXAU generates a non-delivery notificaton	
B.15	Converted indication	Ignore	
B.18	Cross referencing indication	Display in message heading	Reference ⟶ <value>
B.21	Delivery notification	The PTLXAU shall send a delivery notification to the originator	
B.22	Delivery time stamp indication	Ignore	
B.25	Disclosure of other recipients	Disclose all recipients	
B.26	DL expansion history indication	Ignore	
B.29	Expiry date indication	Display in message heading	Message invalid after: ⟶ <value>
B.31	Forwarded IP-message indication	the PTLXAU shall build a message heading for each IP-message contained in the body part	
B.32	Grade of delivery selection	National matter	
B.34	Implicit conversion	Convert to telex according to Rec. X.408	
B.35	Importance indication	Display in message heading	Message importance: ⟶ <value>
B.37	IP-message identification	display in message heading	Message reference ⟶ <value>
B.38	Language indication	Ignore	
B.39	Latest delivery designation	National matter	

TABLE B-1/F.421 *(cont.)*

References Rec. F.400 Annex B	Elements of message	Action to be taken	Examples
B.41	Message identification	Ignore	
B.45	Multi-destination delivery	Deliver the message to all recipients	
B.46	Multi-part body	Messages containing not supported body parts are not delivered. Send back a non-delivery notification to the originator	
B.47	Non-delivery notification	The PTLXAU shall generate a delivery report	
B.48	Non-receipt notification request	Ignore	
B.52	Obsoleting indication		Obsoletes: ⟶ <value>
B.54	Original encoded information types indication	Ignore	
B.55	Originator indication	Ignore	
B.56	Originator request alternate recipient	National matter	
B.62	Primary and copy recipients indication	Display the O/R descriptor information of the recipient(s) in the message heading	TO: ⟶ <value> TO: ⟶ <value> CC: ⟶ <value> CC: ⟶ <value>
B.63	Probe	National matter	
B.67	Receipt notification request indication	Ignore	
B.72	Reply request indication	Display in message heading	Reply ⟶ requested ⟶ by ⟶ sender
B.73	Replying IP–message indication	Display in message heading	Reply to message: ⟶ <value>
B.80	Sensibility indication	Display in message heading just above text of body	
B.88	Subject indication	Display in message heading just above text of body	Subject: ⟶ <value>
B.89	Subsmission time stamp	Display in message heading	Submitted: ⟶ <value> ⟶ UTC
B.90	Typed body	Ignore	

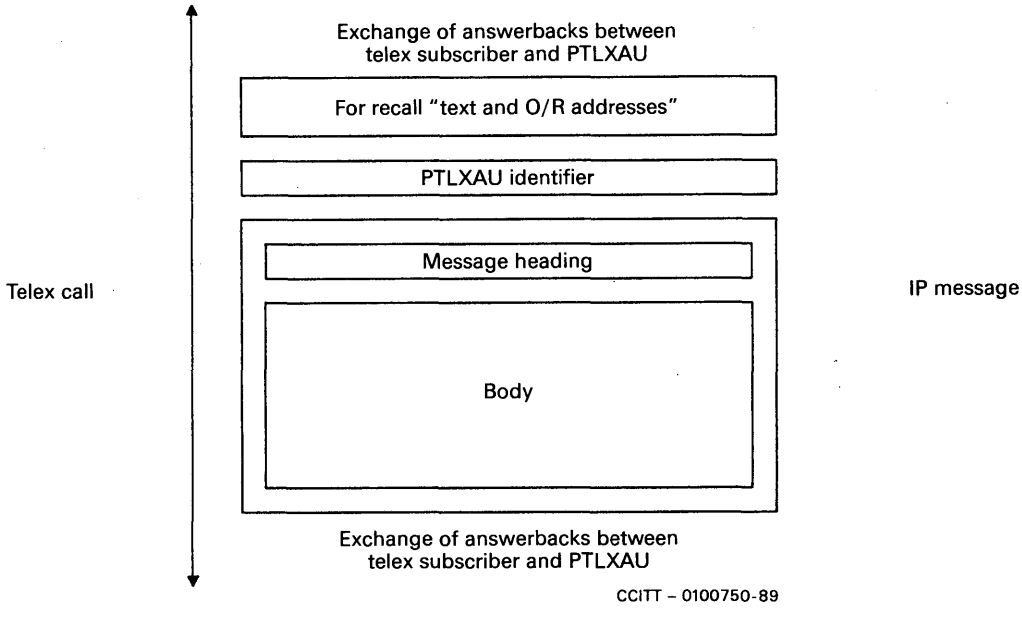
Note – The symbol ⟶ equals a space.

ANNEX C

(to Recommendation F.421)

IPM message to telex

General layout of a message originated by an IPM service user and delivered by the PTLXAU to a telex subscriber.



Display of the originator O/R address related information to the telex user in the message heading:

a) Two-stage selection:

FROM: → GIV → francois
SUR → maurer
ORG → swiss→ ptt
ADM → arcom400
CTN → ch

b) *One-stage selection* :

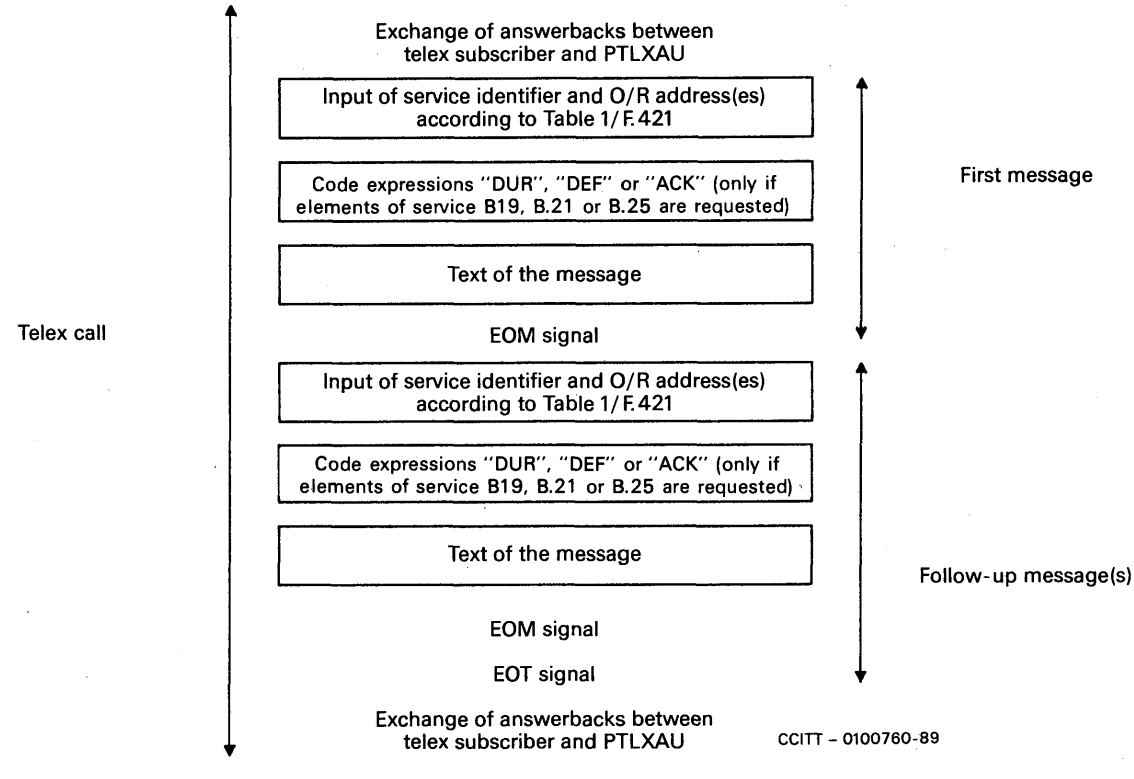
FROM: → (F.74 A/B)

ANNEX D

(to Recommendation F.421)

Telex message to IPM
(Two-stage selection)

General layout of a message originated by a telex subscriber using the two-stage selection, submitted to the PTLXAU for delivery to the IPM service.



MESSAGE HANDLING SERVICES: INTERCOMMUNICATION BETWEEN THE IPM SERVICE AND THE TELETEX SERVICE

The establishment in various countries of message handling services in association with public networks creates the need to produce Recommendations covering the aspects of public message handling services.

The CCITT,

considering

(a) the need for public message handling services;

(b) the strategic and commercial importance of standardization of message handling services;

(c) the urgent need for intercommunication arrangements for existing telematic services, and other services with public message handling services;

(d) the need for a clear distinction between the responsibilities to be allocated to service providers and those of subscribers and/or users;

(e) the need for establishing international compatibility between different messaging systems;

(f) the growth of the installed base of terminals and personal computers with the ability to access message handling systems;

(g) that several F-series Recommendations describe public message handling services;

(h) that certain X and T-series Recommendations cover relevant aspects of systems used for the provision of messaging services;

(i) that the F.200 series and appropriate T-series Recommendations define, respectively, the service and technical requirements for the teletex service;

(j) that Recommendation T.330 defines the technical requirements of the intercommunication between the IPM service and the teletex service,

unanimously declares the view

that where Administrations provide international intercommunication between the public interpersonal message service and the teletex service the operational and service procedures shall be in accordance with this Recommendation.

TABLE OF CONTENTS

1 Purpose and scope

1.1 This Recommendation defines the intercommunication between the public IPM service and the teletex service (for teletex users not registered in the IPM service) and further defines the capability of IPM users to direct messages to teletex users, and teletex users to direct messages to IPM users.

The technical requirements for this intercommunication are specified in Recommendation T.330.

1.2 Teletex users who are registered users of the IPM service are not covered by this Recommendation (see Recommendation F.420).

1.3 For intercommunication the following principles apply:

a) The basic intercommunication function is to allow the exchange of messages from users of one service to users of the other service. The IPM elements of service available to users in each service to intercommunicate with each other are those listed in § 4.

b) Where two Administrations have an IPM service, the preferred method of international intercommunication is through the use of these services.

c) For those Administrations which do not provide an IPM service, in these cases, international connections between the teletex terminal equipment and the public teletex access unit (PTTXAU) should use the international data transmission facilities used for the teletex service.

Figure 1/F.422 shows the environment for the service intercommunication described in this Recommendation.

2 Description of intercommunication

2.1 *Responsibility boundaries*

2.1.1 *IPM service to teletex service*

The PTTXAU retains the responsibility of the message originated by an IPM user until the teletex terminal equipment positively acknowledges the end of the document (see Recommendation T.62).

2.1.2 *Teletex service to IPM service*

The PTTXAU assumes responsibility for a teletex document when it acknowledges the end of the document. The responsibility of the PTTXAU within the MHS is defined in Recommendation F.420.

Identification of the calling teletex terminal is a national matter.

2.1.3 All notifications except receipt notifications are the responsibility of the PTTXAU.

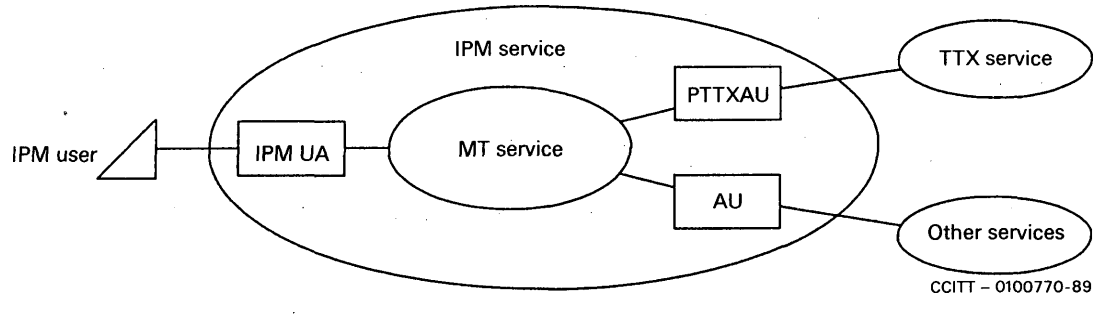


FIGURE 1/F.422

IPM/TTX service intercommunication environment

2.2 *Location of the PTTXAU*

2.2.1 For international intercommunication between the IPM service and the teletex service, the PTTXAU may be located either in the country of origin or the destination country as shown in Figure 2/F.422. If an Administration provides both the IPM service and the teletex service (with a PTTXAU) the international link may be via the MHS.

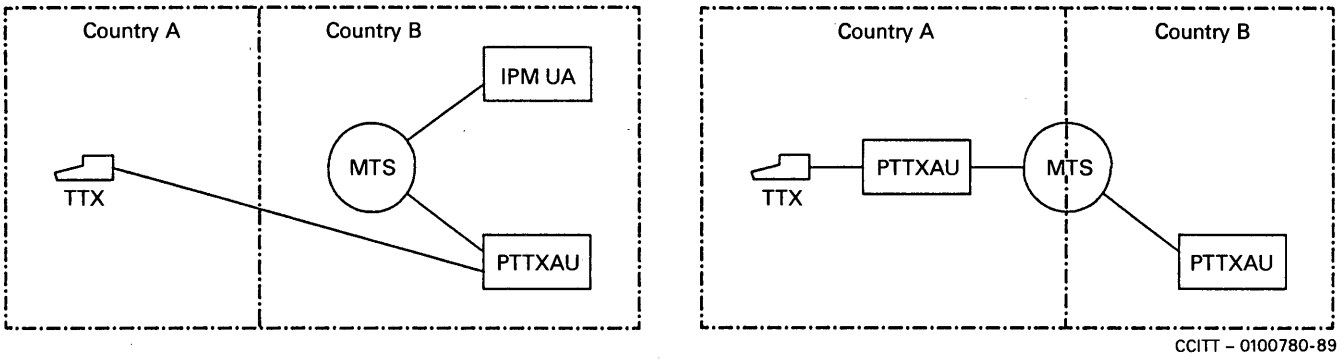


FIGURE 2/F.422

Location of the PTTXAU

3 Requirements for intercommunication

3.1 The intercommunication between IPM service and teletex service and vice versa is based on store-and-forward principles. There is neither interactive nor direct user-to-user communication.

3.2 *Intercommunication from IPM service to teletex service*

3.2.1 When sending an IPM user originated message to a teletex terminal equipment the following conditions may occur:

a) the message can be delivered without conversion;

b) the message can be delivered with conversion;

c) message delivery will not occur because of conversion prohibition;

d) conversion should not be carried out since loss of information beyond that specified in Recommendation X.408 will occur.

3.2.2 Recommendation F.420 applies between the IPM UA and the PTTXAU.

3.2.3 The terminal O/R address of the teletex user as defined in Recommendation F.401 will be used to route the message to the teletex terminal via the appropriate PTTXAU.

3.2.4 The PTTXAU will format IP-messages into documents suitable for delivery to teletex terminal equipment in accordance with Recommendation F.200.

3.2.5 The call identification line (CIL) will contain sufficient information to advise the teletex user of the network address of the PTTXAU.

3.2.6 The header of the message will contain sufficient information in human readable form regarding the originating IPM user.

3.3 *Intercommunication from teletex service to IPM service*

3.3.1 The intercommunication between teletex terminal equipment and the PTTXAU is according to Recommendation F.200. The submission will consist of a document with a formatted header. This header will contain the O/R address(es) and control information related to the IPM elements of service set as specified in Table 1/F.422, and selected by the originator. The format rules are specified in Recommendation T.330.

3.3.2 This formatted header is mapped by the PTTXAU into the envelope and heading necessary for delivering the IP-message to the recipient(s) via the MT service. This process is depicted in Figure 3/F.422. The submission will consist of a heading and body which are mapped into an IPM envelope, heading, and a body.

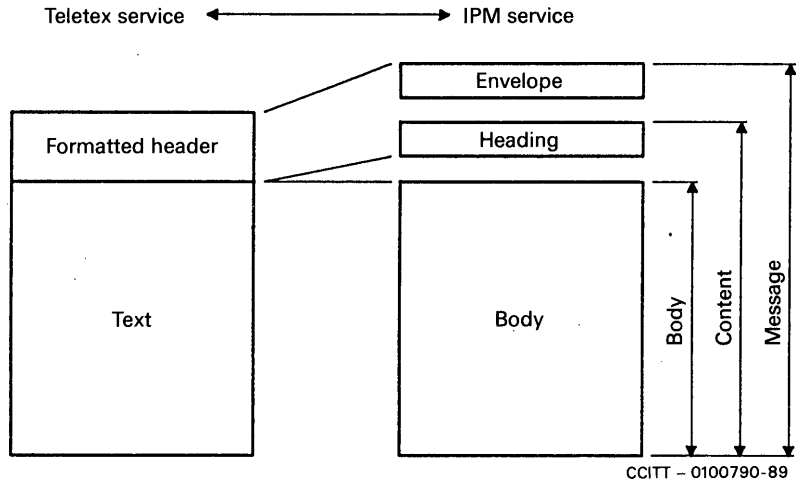


FIGURE 3/F.422

Comparison of a teletex document with an IP-message

4 Elements of service

4.1 The elements of service applicable to IPM/TTX service intercommunication are identified in Table 1/F.422. These are the only elements of service that will be supported in this intercommunication.

5 Quality of service

5.1 Provision of intercommunication should maintain as much as possible the quality of each service.

5.2 The PTTXAU shall be capable of supporting the basic requirements of the teletex terminal equipment as defined in Recommendation F.200. The support of standardized optional user facilities is for further study.

5.3 The PTTXAU will recover from an intercommunication failure with teletex terminal equipment using the document retransmission method.

5.4 If non-delivery notifications cannot be delivered via the normal route it is the responsibility of the Administration providing the PTTXAU to advise the originator via other suitable means.

TABLE 1/F.422

Elements of service

Reference Rec. F.400 Annex B	Elements of service	Message submission from TTX to PTTXAU	Message delivery to TTX from PTTXAU	Information generated by PTTXAU
B.5	Autorizing users indication		X	
B.6	Auto-forwarded indication		X	
B.8	Blind copy recipient indication		X	
B.9	Body part encryption indication		X	
B.12	Content type indication		X	X
B.13	Conversion prohibition	X	X	
B.15	Converted indication		X	
B.18	Cross referencing indication		X	
B.21	Delivery notification	X	N/A	X
B.22	Delivery time stamp indication		X	X
B.25	Disclosure of other recipients		X	X
B.26	DL expansion history indication		X	X
B.29	Expiry date indication		X	
B.31	Forwarded IP-message indication		X	
B.32	Grade of delivery selection	X	X	
B.34	Implicit conversion		N/A	X
B.35	Importance indication		X	
B.37	IP-message identification		X	X
B.38	Language indication		X	
B.39	Latest delivery indication		N/A	X
B.41	Message identification		X	
B.45	Multi-destination delivery	X	N/A	
B.46	Multi-part body		X	
B.47	Non-delivery notification		N/A	X
B.48	Non-receipt notification request	X	N/A	
B.52	Obsoleting indication		X	
B.54	Original encoded information types indication			X
B.55	Originator indication		X	
B.56	Originator request alternate recipient		X	
B.62	Primary and copy recipients indication	X	X	
B.72	Reply request indication		X	
B.73	Replying IP-message indication		X	
B.80	Sensitivity indication		X	
B.88	Subject indication	X	X	
B.89	Submission time stamp indication		X	X

Note – Definitions of the Elements of Service are contained in Recommendation F.400, Annex B.

ANNEX A

(to Recommendation F.422)

Abbreviations

AU	Access Unit
CIL	Call Identification Line
DL	Distribution List
IPM	Interpersonal Messaging
MHS	Message Handling System
MT	Message Transfer
MTS	Message Transfer System
N/A	Not Applicable
O/R	Originator/Recipient
PTTXAU	Public Teletex Access Unit
TTX	Teletex
UA	User Agent

Note 1 – For a glossary of terms see Annex A to Recommendation F.400.

Note 2 – For references see Recommendations F.400 and F.401.

PAGE INTENTIONALLY LEFT BLANK

PAGE LAISSEE EN BLANC INTENTIONNELLEMENT

SECTION 2

DIRECTORY SERVICES

Recommendation F.500

INTERNATIONAL PUBLIC DIRECTORY SERVICES

Given the rapid multiplication and expansion of CCITT-defined telecommunication services, there is a growing need for subscribers to these telecommunication services to be able to communicate with each other. In order to facilitate such intercommunication for the subscribers of the various services, public directory services will be required.

The CCITT,

considering

(a) that the CCITT-defined telecommunication services, including Telegraphic, telematic and telephone services, have directory requirements;

(b) that such requirements are being implemented as on-line electronic directories (in addition to traditional hard-copy versions);

(c) that national initiatives are being taken to develop electronic integrated directories or service specific directories;

(d) that the system definition is being undertaken by the CCITT in the field of electronic directories in the X.500-series of Recommendations,

unanimously declares

that the specifications of this Recommendation should be applied to the provision of public directory services.

CONTENTS

1 Introduction

International public directory services will enable subscribers to determine rapidly and easily what services are available and how to access and address their correspondents. Public directories may also be used internally by the various telecommunication services for the proper routing of calls or messages. However, this application of directory systems is not covered by this Recommendation.

Service specific directories may be implemented as part of a global directory service. Consistent with the need to make directory information as widely available as possible, it is anticipated that Administrations will aim to provide global electronic directory services.

In order to provide international public directory services, Administrations should mutually cooperate in handling inquiries for information across national boundaries.

Public directory services should solve the primary problem of name to address association, e.g. obtaining a company's telex number by querying the directory with the name of the company. The reverse question, i.e., obtaining the name and other information from the address, may also be applicable in certain services and its provision is at the option of an Administration.

Public directory services should include directory information concerning the provision of services, service descriptions, operational instructions, tariff conditions, etc.

Public directory services should make provision for accessing information without knowing the name of the object sought, e.g., designating categories of goods, business areas or services.

Advertising is included in the scope of public directory services, but is left to national implementations.

Public directory services can be considered as supplementary to the services for which they provide information or by which they are accessed.

Private directory services which are compliant with the public directory services defined in CCITT Recommendations may be permitted to intercommunicate with public directory services under national regulations.

2 Purpose and scope

This Recommendation provides for the general framework for the provision of international public directory services. It defines the requirements for and the service features associated with the provision of public directory services. It specifies naming aspects, describes operational issues to be taken into account in providing the public directory services as well as quality of service aspects.

3 Organizational provisions

Provision of a public directory service will be done in accordance with the organizational model described in Recommendation X.501. An Administration Directory Management Domain (ADDMD) is responsible for the application of the basic service features and the optional user facilities provided in that domain. Directory management domains shall intercommunicate with each other as far as the provision of the public directory services requires it. The protocol to be used for interworking as well as the directory's overall concept and behavior, is described in the X.500 series of Recommendations.

Private Directory Management Domains (PRDMDs) may exist and intercommunicate with ADDMDs, following national regulations.

A Directory Management Domain (DMD) consists of one or more Directory System Agents (DSAs) and zero or more Directory User Agents (DUAs).

Each directory management domain may act as the naming authority for that domain. Names need to be unambiguous.

The intercommunication between PRDMDs is *outside* of the scope of this Recommendation.

4 Public directory services

4.1 *Service requirements*

The fundamental ability of a public directory service is to provide a means by which subscribers or users of telecommunication services may, in a user-friendly manner, and from information they would normally possess, obtain information about a desired recipient, such as addresses or communication capabilities.

This public directory service is provided in an on-line and interactive manner. It should be made available for subscribers or users at the discretion of the Administration offering the service.

Each Administration is responsible for the access methods used. The characteristics of the access methods between terminals and the public directory service are a national matter. However, the directory service offered is independent of the access method, the terminal used and the location of the user.

Public directories of Administrations should intercommunicate (or refer to each other) to fulfill requests made by customers when the directory serving the customer does not have available the information requested.

4.1.1 *Basic service requirements*

The following basic service requirements are fulfilled by the public directory services:

- to provide subscribers with information, e.g., a telex number, needed for establishing communication with other subscribers or users of telecommunication services;
- to provide subscribers with information, e.g., service instructions, needed to use the telecommunication services and the directory itself;
- to assist subscribers in the formulation of queries to narrow the scope of the operation;
- to allow for flexibility in the formulation of a request, e.g., names should not artificially remove natural ambiguities; names should admit natural abbreviations and commonly used variations in spelling.

4.1.2 *Non-basic service requirements*

The following non-basic service requirements are fulfilled by the user facilities of the public directory services.

- to provide subscribers with other information, e.g., advertising;
- to provide subscribers with "yellow page" information, e.g., categories of goods, business areas or services;
- to provide an interted directory for specific services, e.g., for telex and teletex;
- to provide "wildcards" capability to ease, as far as possible, the input of the requests to the directory;
- to provide means for the verification of credentials, under conditions specified by the provider of the directory service;
- to provide possibilities for the search of distribution lists;
- to provide means for the phonetic matches.

4.2 *Service features and optional user facilities*

The service features and the optional user facilities of a public directory service will be provided in accordance with the X.500-series of Recommendations. The terms used in the context of service features and optional user facilities discussed below are explained in Annex H.

4.2.1 *Basic service features*

Basic service features are *inherent* in directory services and are always available for use in directory service. They are provided by *all* service providers offering international public directory services or by private directories intercommunicating with public directory services.

The basic features are:

- read operation;
- search operation.

Other basic features are for further study.

4.2.2 *Optional user facilities*

Optional user facilities may be selected by the user or subscriber at the time the service is being used. Each optional user facility visible to the user is classified as either essential or additional. Essential (E) optional user facilities *are* to be made available internationally by Administrations. Additional (A) optional user facilities *may* be made available by Administrations for national use and for international use on the basis of bilateral agreement.

The major terms used in this Recommendation are contained in Annex H.

The classification of optional user facilities is shown in Table 1/F.500.

TABLE 1/F.500

Classification of optional user facilities

	Classification
Abandon	E (see Note 1)
Add	A
Additional service controls	A
Compare	A
Distribution lists	A
List	A
Management of access control	A (see Note 2)
Modify	A
Remove	A
Security capabilities	A
Time limit service control	E

Note 1 – This abandon operation is not guaranteed outside of the local scope, i.e., the DSA or DMD to which the original request was made.

Note 2 – The full functionality is presently not provided in the present system specification of the X.500 series of Recommendations (see X.501, § 3 and Annex F). This is for further study and referred to as being presently a national matter. Access control functions are for further study.

Other optional user facilities are for further study.

4.3 *Further features and facilities*

Some of the following items are not yet specified as elements of service in the X.500 series of Recommendations and will be studied further. Some others will need further study under service aspects. The following list may provisionally be considered as guidance for service providers to be taken into account for the provision of public directory services under national responsibility. The items may become basic features or optional user facilities in the future or/and will be included with descriptive text in future Recommendations.

- Provision of inverted directories for telex and teletex services.
- Provision of additional information with or after the result of a query.
- Provision of query cost information.
- Provision of information about services, service instructions, tariffs, etc., in standardized formats taking into account additional attributes.
- Provision of additional service controls.
- Provision of full functionality of access control mechanisms.
- The ability of the user to indicate the desire not to receive partial results when service control maximum parameters are exceeded.
- Provision of the return of multiple responses in groups of n (n = any number).
- Provision of administrative procedures for authentication.
- Provision of standardized error service messages.
- Provision of shadowing (controlled replication) of directory information.
- Provision of geographical extension.
- Consequences of distributed directory services.

4.4 *Service controls*

Because of its generality and scope, the direcory service can fulfill subscribers' requests that might require consumption of resources beyond a level desired by the subscriber or by the service provider. Service controls help to prevent such situations by imposing limits on the resources that may be consumed in fulfilling a request for service. Service controls not impacting the provision of international directory services are a local matter. The following service controls are provided by the system application (see Recommendation X.511):

4.4.1 *Prefer chaining*

This service control indicates a choice for chaining over referral and multicasting. For the international intercommunication of public directories, chaining is the preferred choice.

The setting of this service control is for the service provider who may allow the user to invoke it.

4.4.2 *Chaining prohibited*

The scope of a search will then be limited to the local portion of the Directory Information Base (DIB) by prohibiting chaining.

The setting of this service control is for the service provider who may allow the user to invoke it.

4.4.3 *Local scope*

The scope of the operation will be limited to the local portion of the DIB. The determination of local is restricted to a single DSA or DMD in accordance with an Administration's policy.

For the international intercommunication of public directories, generally no limitation to local scope is assumed. Public directories will aim to open their scope as much as possible. The setting of this service control is for the service provider who may allow the user to invoke it.

4.4.4 *Do not use copy*

This service prevents a DMD from returning copied information.

The setting of this service control is for the service provider who may allow the user to invoke it.

4.4.5 *Do not dereference alias*

This service control allows reference to an alias entry itself rather than to the aliased entry.

The setting of this service control is for the service provider.

4.4.6 *Priority: low, medium, high*

The setting of this service control is for the service provider.

The usefulness of this service control is for further study.

4.4.7 *Time limit*

The scope of this service control is to limit an operation in terms of total elapsed time such that if the limit is exceeded, then the operation will be terminated, and for search and list operations partial results should be returned, with the indication that results are incomplete due to the time limit. This service control *shall* be honoured by any DMD involved.

The setting of this service control is for the service provider who may allow the user to invoke it.

Note – This service control is an essential optional user facility. All service controls other than the time limit are a local matter and when implemented, need not be made available by the service provider to the user.

4.4.8 *Size limit (applicable to search or list operations)*

If the list size specified is exceeded any results equal in number to the size limit should be returned, with the indication that the results are incomplete due to the size limit.

The setting is for the service provider who may allow the user to invoke it.

4.4.9 *Scope of referrals*

Indicates the scope to which a referral (or advice), if generated, is to be restricted to, i.e., limits the range of alternate access points at which the requestor (DUA or DSA) may alternately use to satisfy the request. The limitation can be restricted to a country or DMD.

The setting of this service control is for the service provider who may allow the user to invoke it.

Note – Combination of some service controls may affect the quality of the results, e.g., combination of priority, time limit and size limit may conflict, or chaining cannot be both preferred and prohibited simultaneously. If no service controls are supplied with an operation, the following is assumed: referrals and/or chained operations may be used; no limit on the scope of the operation; locally held copies of information are permitted; no preference of priority for operation processing; there is no time or size constraint; referrals, if generated, are not restricted to a DMD or country; and aliases are dereferenced.

5 Names as the key to directory searches

5.1 *General*

A *name* within the directory service is a label which is constructed to identify a particular object, that is, which singles out an object from the set of all objects. A name should not be ambiguous, that is, should *not* denote more than one object. However, there may be more than one name for an object. Thus, it is possible to call an object by the name *International Widget Makers* or IWM. In either case, one and only one object is identified.

A more abstract definition of "name" can be found in Annex H.

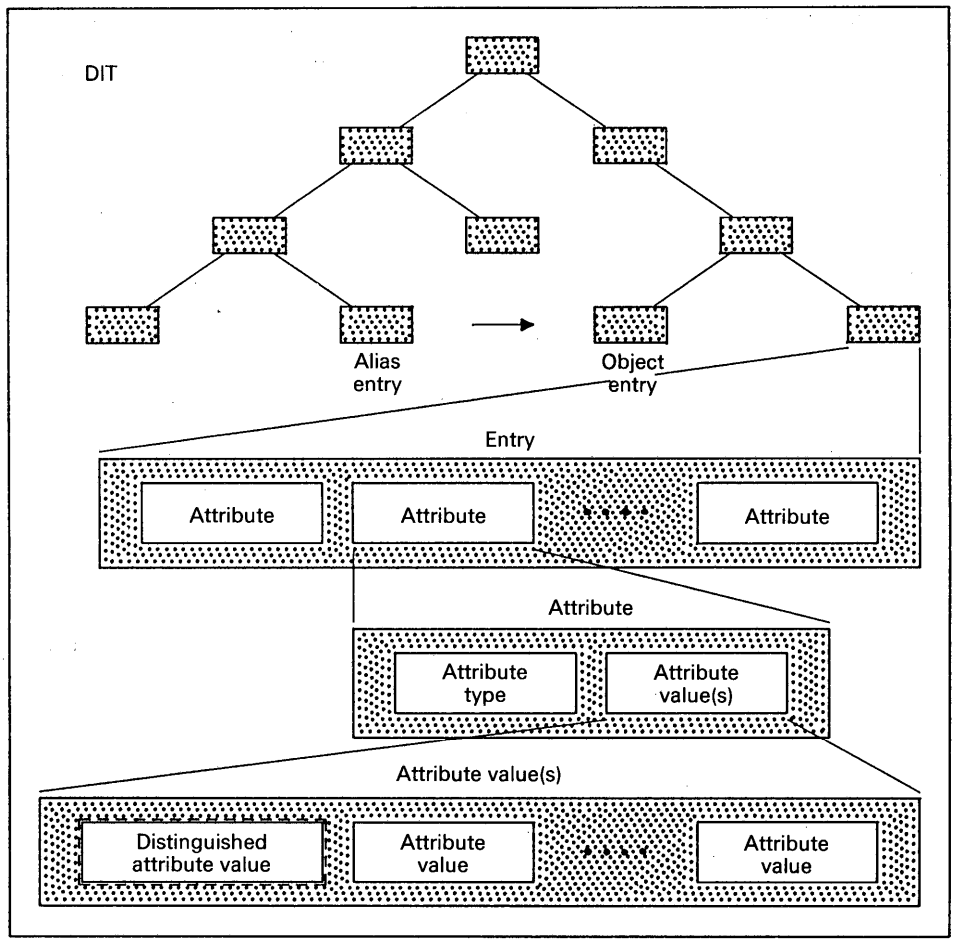
5.2 *Entries*

The directory service will provide information about entries. The complete set of such information is called the Directory Information Base (DIB). The information about entries is composed of attributes; attributes, in turn, are composed of an attribute type (one type of attribute could be a telex number) and one or more attribute values. (The actual telex number would be a value.) The entries are arranged in a tree, called the Directory Information Tree (DIT). This is graphically illustrated in Figure 1/F.500. However, this does not preclude other directory information structures.

Thus, an entry may be viewed as an entity which is named through one or a series of attributes. A company may be sufficiently named simply through the use of its actual legal name e.g., the PADRAIC STEEL CO. A plumber in Secausus, N.J. can be named through the use of his common name, his postal address and his business category "plumber". A human person may be named through the use of his or her common name and telephone number.

5.3 *Distinguished names*

It should be noted that within the directory system recommendations, the term "distinguished name" is used. This is the combination of the minimum attribute value assertions (AVAs) needed to denote an entry uniquely. This minimum will be established in accordance with the requirements of the naming authority and/or the directory management domain, and the preference of the owner of tne entry named. Use of the distinguished name may be of assistance in performing the most effective search of the DIB. However, it should be recognized that in some instances, distinguished names may not be user friendly and may contain information, which, in fact, is the object of the directory search, i.e., a person's postal address.



Note 1 – The Alias entry has a pointer to the actual entry for which it is the alias and does not contain the actual object information.

Note 2 – See also Recommendations of the X.500 series.

FIGURE 1/F.500

Structure of an entry in a directory

5.4 *Classification of requests*

To satisfy the most common needs of directory users which are presently met by so-called "white pages" or "yellow pages" (classified directories) or organization directories, three classifications of requests to the directory service are provided.

5.4.1 *Common name requests (type 1)*

Information returned under this type of request includes information about one or more of the following entries. (Selected object classes can be found in Recommendation X.521; they are listed in Annex C.)

a) A person

Example: Bernadette L. Casey

b) A residential person

Example: Cornelius Fecit
2 Humbug Road
Fun City, New York 11666
USA

c) An application entity

Example: Some logical name, usually a sequence of alpha and/or numeric characters identifying an application process; consequently not necessarily user friendly.

d) A communication device

Example: the XYZ 9.6 modem (however, this information is normally associated with an organization and is thus generally of greatest utility to organizations).

e) An alias

Example: Neil Fecit [an alias for the residential person in b)]

f) An organizational role

Example: Director of regulatory affairs

g) A group of names

Example: Members of special rapporteur's group Question 14/1.

5.4.2 *Business category requests (type 2)*

Information returned under this type of request includes information about one or more of the following entries. (Selected object classes can be found in Recommendation X.521; they are listed in Annex C.)

a) A person

Example: John Smith

b) A residential person

Example: John Smith, with the rest of the postal address

c) An organization

Example: The Padraic Steel Company

d) An organizational unit

Example: Regulatory Affairs Department

e) A group of names

Example: The plumbers in Secausus

5.4.3 *Organization requests (type 3)*

Information returned under this type of request includes information about one or more of the following entries. (Selected object classes can be found in Recommendation X.521; they are listed in Annex C.)

a) An organization

Example: The Padraic Steel Company

b) An organizational unit

Example: Regulatory Affairs Dept.

c) An organizational person

Example: John Jones, Padraic Steel Company

d) An organization role

Example: Chief Operating Office

e) A group of names

Example: The President's Staff

f) An application entity

Example: as above in § 5.4.1 c)

g) A device

Example: An XYZ 9.6 modem

h) An organizational unit alias

Example: the "bean counters" which is an alias for the "Controller's Dept."

i) An organizational name alias

Example: GMC for "Good Modern Cooks Inc."

5.4.4 *Use of attributes*

Attribute types that are recommended to be included, whenever they exist (subject to the permission of the owner) in each entry of each group, either for query or retrieval, are listed in Table 2/F.500 (see also Annex D).

TABLE 2/F.500

Use of attributes for each type of request

Attribute type	Abbreviation	for Type 1	for Type 2	for Type 3
Business category	BCTG	–	M	R
Common name	COM	M	Q	Q
Country name	CTN	M	M	M
Description (free text)	DES	R	R	R
Destination indicator (public telegram)	DI	–	–	–
Facsimile telephone number	FAX	–	Q	Q
ISDN address	ISDN	–	Q	Q
Knowledge information	KI	–	–	–
Locality name	LOC	M	Q	Q
Member	MEM	R	R	R
Object class	CLASS	Q	Q	Q
O/R address (MHS) (see Note 1)	O/R	R	R	Q
Organization name	ORG	–	–	M
Organizational unit name	OUN	–	–	Q
Owner	OWN	–	–	–
Physical delivery office name	PDO	Q	Q	Q
Post office box	POB	Q	Q	Q
Postal address	PADD	Q	Q	Q
Postal code (see Note 2)	PCOD	Q	Q	Q
Preferred delivery method	DLM	R	R	R
Presentation address	PRADD	R	–	R
Registred address (public telegram)	RADD	–	R	R
Role occupant	RO	R	–	R
Search guide	SG	R	R	R
See also	SEE	R	R	R
Serial number	SN	–	–	–
State or province name	STN	M (see Note 3)	Q	Q
Street address	SADD	Q	Q	Q
Supported application context	SAC	Q	Q	Q
Surname	SUR	Q	Q	Q
Telephone number	TEL	Q	Q	Q
Teletex terminal identifier	TTX	R	Q	Q
Telex answerback (see Note 4)	A/B	R	R	R
Telex number	TLX	R	Q	Q
Title	TIT	–	–	Q
User certificate	UC	R	R	R
User password	UP	R	R	R
Videotex user number (see Note 4)	VTX	Q	Q	Q
X.121 address	X.121	–	Q	Q

Note 1 – This attribute type is defined in the X.400 series of Recommendations.

Note 2 – The postal address will normally contain the postal code. Requirements may exist to justify the postal code as being a separate attribute type. Specific conditions are applied to a postal address for Physical Delivery (see Recommendation F.401).

Note 3 – Depending on the value of the attribute "CTN".

Note 4 – This attribute type has not yet been defined in Recommendation X.520.

M Mandatory to *reach* an object of this type.

Q May be used to reach an object of this type (within a distinguished name or as a search filter), but may also be part o the directory response. Additional attribute types may be used for selection criteria within national implementations.

R Normally part of the directory response with regard to the request of the user.

– This attribute type may either be part of a local sub-object class or used nationally.

Some terms used in Table 2/F.500 are explained in Annex H. Definitions of other terms can be found in the X.500 series of Recommendations.

5.5 *Naming of entries*

To reach an entry, a user has to provide some information, a part of which is essential to the performance of the request (e.g., the provision of attributes CTN, ORG, CLASS, for an organizational object), as described in § 5.2.

Depending on the knowledge the user has about the naming structure of the part of the directory information tree (DIT) to which the entry of the intended object belongs, the request information provided by this user to reach the intended entry is either the distinguished name of the entry (in which case the response is unique), or the value of some relevant search attributes (already known by the user) arranged in a logical pattern to act as a filter to reduce as far as possible the number of the directory responses.

Since distinguished names have to be unambiguous, it is not expected that they will always be user-friendly. For instance, a name of a residential person may include the telephone number and thus be rather difficult to predict, especially if the telephone number is the information requested from the directory. It is recognized that the distinguished name (DN) of an object may not be commonly known, in which case the DN may be acquired by using a list operation and in some instances a search operation.

To perform efficiently the search or list operation, it is recommended that one narrows as far as possible the scope of the search, either by giving a base object (from which the search starts in the DIT) near enough to the intended entry (in terms of DIT levels), or by obtaining and using the appropriate filtering.

It should be possible to obtain from the directory which of the attributes (qualified with "Q" in Table 2/F.500) may be used as part of the search filter for a given object class starting from a given base object. However, it is recognized that the use of this feature across domain boundaries is subject to national restrictions and bilateral agreements.

It is expected in most cases that a directory management domain will be able to provide from previous experience the useful search criteria of subordinate levels, whether or not they efficiently manage those levels, without exploring the DIT further for each request. Knowledge of the search criteria may also be acquired by DUAs from the directory by automatic means, e.g., by reading the "search guide attribute" if available.

It is up to the Directory Management Domain (DMD) managing a given entry to select from the attribute types specified in § 5.4 for use as search criteria.

The use of wildcards to replace the value or part of the value of unknown recommended search criteria should be made possible.

Phonetic or orthographic extensions, when requested, may be *locally* applied to the provided values for query operations. However, their actual provision depends on the capabilities of the directory system. The fall-back mode is phonetic or orthographic extensions not supported.

5.6 *Qualifications of attribute types*

Some criteria of the selected attribute types require qualification.

"Mandatory" in Table 3/F.500 indicates that, if *that* attribute type exists in an entry of the directory, it shall be part of any response provided, when asked for by the user, and that no combination of access controls may be kept on attributes which would preclude provision of a meaningful directory service, subject to the owner's approval.

The "required length" of an attribute type in Table 3/F.500 designates the minimum number of character positions to be made available for the attribute type to be displayed on the terminal of a user, and can therefore assist Administrations in defining their attribute values with the assurance that the attribute value will not be truncated. (The X.500-series Recommendations have system qualifications for the maximum length of attribute types.)

The system specification does not provide multiple values for country name and preferred delivery method. All others may be recurring. For example, an organization may be "Padraic Steel" and "Padraic Steel Company". Only one value needs to be displayed to the user.

Table 3/F.500 contains a list of the user-visible selected attribute types to be used in the directory service. The figures shown may require revision in the light of experience.

TABLE 3/F.500

Qualifications of attribute types

Attribute type	Mandatory	Required length
Business category	Yes	128
Common name	Yes	64
Country name (see Note 1)	Yes	30
Description	Yes	1024
Destination indicator (public telegram)	Yes	4
Facsimile telephone number	No	150
ISDN addresse	No	16
Knowledge-information	No	–
Locality name	Yes	64
Member	No	–
Object class	No	–
O/R address MHS (see Note 2)	Yes	–
Organization name	Yes	64
Organizational unit name	Yes	64
Owner	No	–
Physical delivery office name	No	64
Post office box	No	40
Postal address	No	180
Postal code (see Note 2)	No	20
Preferred delivery method (see Note 3)	Yes	15
Presentation address	No	–
Registered address (public telegram)	Yes	60
Role occupant	No	–
Search/Guide	Yes	–
See also	Yes	–
Serial number	No	64
State or province	Yes	64
Street address	No	64
Supported application context	No	–
Surname	No	64
Telephone number	No	16
Teletex terminal identifier	No	24
Telex answerback (see Note 2)	No	21
Telex number (see Note 3)	No	36
Title	No	64
User password	No	–
User certificate	No	–
Videotex user number (see Note 2)	No	17
X.121 address	No	15

Note 1 – The system specification provides only a 2-character length, to correspond to the ISO 3166 value.

Note 2 – The postal address will normally contain the postal code. Requirements may exist to justify the postal code as being a separate attribute type. Specific conditions are applied to a postal address for Physical Delivery (see Recommendation F.401).

Note 3 – The system specification provides a shorter field.

Note 4 – For some attribute types, values are stored in encoded/compressed format and will need to be displayed in a non-encoded format or human readable format.

Note 5 – See also Recommendation X.520, Annex C.

6 Character repertoire and languages

6.1 *Character repertoire*

Directory information will be entered and stored locally using a character repertoire suitable to the country where the directory is located. More than one character repertoire may be needed to cover different languages or to provide for access from different types of communication terminals.

However, in order to provide international public service, the character repertoire to be used internationally should be limited to CCITT standardized sets, i.e., the IA5 and T.61 character repertoires.

For the intercommunication between public directory services, the repertoires may be agreed to bilaterally.

However, where no such agreement exists, the character repertoire to be used shall consist only of those characters defined as "printable string" in Recommendation X.208. Furthermore, those Administrations which use character reportoires other than this repertoire shall provide suitable conversion of the information into this character repertoire for directory requests from Administrations with which no bilateral agreement has been reached.

Subscribers have to be instructed on the use of the appropriate character repertoires.

6.2 *Language of requests to the directory and responses from the directory*

Subject to the conditions in § 6.1, the results of requests to the directory should normally be provided in the language or languages of the DMD providing the information. However, the information is presented to the requestor is a national matter.

7 Display of a response

Attribute types and values will be displayed to the user, when required, by converting the values in accordance with Recommendation X.408.

Though it is logical enough that the right response always be sought, in some cases where no such answer can be provided, and on explicit request of the requestor, the directory may also provide phonetic and orthographic extensions corresponding to the intended object.

For displaying directory responses, the following order is recommended:

a) the right answer(s);

b) the answer(s) approaching the right answer(s) using conjunctions, particles, articles, as well as extended or concatenated abbreviations;

c) the phonetic and orthographic extensions (e.g. plural instead of singular denominations). It should be noted that such responses may be erroneous.

Partial responses, including referrals, should be displayed to the requestor and properly identified as such. The cause for partial responses should also be displayed.

8 Operational issues

8.1 *Management*

It is the responsibility of the Directory Management Domains (DMDs) to exercise the management of information within their Domains. Inter-Domain Management is for further study.

8.2 *Authentication*

Authentication in this context means that the identity of the subscriber or user is established. In some cases, the directory service has to ensure that directory information is released only to authorized requestor(s), and in some cases it has to ensure that data is modified only by an authorized originator (e.g., by employing techniques related to data origin authentication).

Checking and keeping of credentials, when performed, are at the discretion of the DMD, taking into account the requirements of privacy of the owner of the information. The precise reason for credential failure will be masked from the user. The user will be advised that denial of the request was because an inappropriate authentication level was encountered.

See also Recommendation X.509.

Further study is required.

8.3 *Access control*

Access controls are a national matter. When access control prohibits the return of the information requested, an appropriate code error code will be returned.

Note – The international application of access control is for further study.

8.4 *Operational actions*

Actions performed within a directory can be categorized as:

1) primary (subscriber/directory) action – always in direct support of a subscriber;
2) secondary action in support of a subscriber request, either serving the subscriber's DUA or an intermediary DSA.

These actions are qualitatively different, and differ also in what they imply concerning the obligations of an ADDMD.

Examples of such interactions can be found in Recommendation X.518.

8.4.1 *Primary (subscriber/directory) action*

The public directory service should provide three user-visible activities of support, as follows:

a) *Request formation*

In this activity, the subscriber composes a request to the directory. The way in which these functions are performed is a national matter.

b) *Presentation of results*

In this activity, the directory service presents to the subscriber the results of a previously entered request. The format, presentation medium and other aspects of result presentation are a national matter.

c) *Subscriber assistance*

In this activity, the directory service assists the subscriber by providing instructions on the use of the directory. The means through which the subscriber asks for such instruction, and the manner in which an instruction is delivered, are a national matter.

8.4.2 *Secondary action for subscriber support*

In order to provide the public directory service, DMDs shall cooperate. Such cooperation includes adherence to defined patterns of interaction, and also includes provision of requested directory information to one another, subject only to internationally agreed access controls (or bilateral arrangements). This technical cooperation among DMDs implies an equivalent level of cooperation in service terms, especially with regard to information sharing, among the DMDs. Examples of such interaction can be found in Recommendation X.518.

8.5 *Maintenance of the directory information*

The service provider has to ensure integrity of the information contained in the directory. Shadowing (controlled replication) of information in other DMDs is *permitted* by bilateral agreement. The international application is for further study.

Creation and modification of directory information by the subscribers may be permitted by the DMDs concerned.

8.6 *Error handling*

Error conditions will be returned as a value of an error code for all standardized operations. The meaning will be displayed according to national implementations as service error messages to the user.

See Annex B/F.500 for guidance.

8.7 *Operator assistance*

For further study.

9 Quality of service aspects

9.1 *Availability*

In principle, a public directory service should be available to subscribers 24 hours a day, seven days a week.

9.2 *Security of directory information*

Information in public directories should be given the broadest dissemination. However, subscribers or users about whom information is available in a directory should be able to require the entity charged with the management of the directory to limit access to such information to ensure their own privacy.

9.3 *Successful directory requests*

Normally, a successful directory request will result in a report of all the requested information, unless it is denied because of authorization restrictions.

Requests to the directory which do not provide sufficient information to execute a reasonable search will normally not lead to a successful result.

9.4 *Access*

Providers of a public directory service should ensure that an adequate number of access ports are available to accommodate subscribers' requests for information. In principle, this means that a requestor will receive a prompt within 15 seconds as a goal.

9.5 *Response time*

Recognizing that responses to requests will be controlled in part by the level of ambiguity tolerated in requests and the number of DMDs which shall be traversed to retrieve the information requested, a subscriber normally should expect an initial acknowledgement regarding his request within 5 seconds. The scope and priority of the request may have an impact on the response time. The requestor may terminate his request at any time.

A final response (successful or unsuccessful) will depend on the capabilities of the directories consulted. A response indicating that no information or incomplete information is available (possibly with hints for further searches) should be given within one minute.

Note – The figures for quality of service are provisional and may be revised in the future.

10 References

10.1 *Recommendations of the X.500 series* – Data communication networks: directory

X.500 The directory – Overview of concepts, models and services

X.501 The directory – Models

X.509 The directory – Authentication framework

X.511 The directory – Abstract service definition

X.518 The directory – Procedures for distributed operation

X.519 The directory – Protocol specification

X.520 The directory – Selected attribute types

X.521 The directory – Selected object classes

10.2 *Recommendations of the X.200 series* – Data communication networks: open systems interconnection (OSI)

10.3 *Recommendations of the F.400 series* – Message handling and directory services operations and definition of service

10.4 *Recommendations of the X.400 series* – Data communication networks: message handling systems

ANNEX A

(to Recommendation F.500)

Abbreviations

A	Additional Optional User Facility
ADDMD	Administration Directory Management Domain
AVA	Attribute Value Assertion
DIB	Directory Information Base
DIT	Directory Information Tree
DMD	Directory Management Domain
DN	Distinguished Name
DSA	Directory Systems Agent
DUA	Directory User Agent
E	Essential Optional User Facility
ITU	International Telecommunication Union
PRDMD	Private Directory Management Domain
RDN	Relative Distinguished Name
RPOA	Recognized Private Operating Agency

ANNEX B

(to Recommendation F.500)

Service error messages

Error codes produced while performing operations in directory systems are transformed by the local DUA into service error messages. The values of the error codes and the meaning are summarized in this Annex. Standardized service error messages are for further study. The presentation to the user is a local manner.

See also Recommendation X.511.

B.1 *Attribute error*

This error is displayed on a per-selection criteria basis (attribute type) and includes the attribute type, attribute value and problem reason value. The problem reason values are as follows (see Table B.1/F.500).

TABLE B-1/F.500

Reason value	Meaning
1	The requested information does not exist for the named entry.
2	The syntax of the value used for the distinguished name or the selection criteria <attribute> is inappropriate. Contact support staff for assistance.
3	Attribute Type <attribute> is not defined for this <object>.
4	Inappropriate matching for the information type <attribute type>.
5	Attribute Type <attribute> or Attribute Value <value> is not within its constraints.
6	<attribute type> or <attribute value> already exists.

B.2 *Name error*

This will be displayed with one of the following reason values whenever a name provided by the user is detected to have a problem (see Table B.2/F.500).

TABLE B-2/F.500

Reason value	Meaning
1	The name supplied, <name>, cannot be found. (*Note* – ALIAS names are resolved to the actual named entry.)
2	<name> is an Alias that can not be properly resolved.
3	Part, <attribute type>, of the name used is underfined.
4	The syntax of the value used, <attribute value>, is inappropriate.
5	List operation is improperly specified.
6	An Alias was encountered in an operation where it is not allowed.

B.3 *Interconnect error*

This error will be displayed whenever the operation cannot be carried further at this time. The possible access points for continuing the request are provided in the form: "Name and Access Point".

B.4 *Service error*

This will be displayed with one of the following reason values whenever the operation requested has detected a problem that affects the user service (see Table B.3/F.500).

TABLE B-3/F.500

Reason value	Meaning
1	The directory system is busy.
2	The directory system is presently unavailable.
3	System is unable to proceed with the request. Contact support staff for assistance.
4	Information not found in the local system. [Optionally, the directory service provider may advise the user that the restriction to use local service information only should be removed and the request may be re-submitted to allow remote directory services to be utlized.]
5	Administrative limit exceeded. Contact support staff for assistance.
6	Unavailable critical extension.

B.5 *Update error*

This will be displayed with one of the following reason values whenever the the modify (Add, Change, or Delete) operation(s) requested has detected a problem (see Table B.4/F.500).

TABLE B-4/F.500

Reason value	Meaning
1	The update violates directory naming rules.
2	The update violates the directory rules for that class of objects.
3	Update not allowed because of the object's position in the directory.
4	Update not allowed on an RDN when modifying an entry.
5	Entry already exists (relevant for add operation only).
6	Update denied, affects multiple directory systems.
7	Any update against this class of objects prohibited.

B.6 *Security error*

For further study.

B.7 *Abandon error*

For further study.

B.8 *Referral error*

For further study.

ANNEX C

(to Recommendation F.500)

Selected object classes

See Recommendation X.521.

Object identifies are allocated to object classes. The concept makes use of the concept of subclasses (see Recommendation X.501).

Selected object classes provided by the directory systems specifications depend on the scope of public directory service chosen by the service provider. It is assumed that the presently defined selected object classes will allow the provision of a useful directory service.

- Top
- Alias
- Country
- Locality
- Organization
- Organizational unit
- Person
- Organizational person
- Organizational role
- Group of names
- Residential person
- Application entity
- Application process
- DSA
- Device
- Strong authentication user
- Certification authority

Note 1 – A certain object class is used as a classificatory attribute type.

Note 2 – The definition of additional selected object classes for public directory service is for further study.

Note 3 – Messaging handling, in X.400-series of Recommendations, defined additional object classes for MHS specific use (see Annex E).

ANNEX D

(to Recommendation F.500)

Selected attribute types

It is assumed that the presently defined selected attribute types will provide a useful directory service. The implementation of the attribute types used in the public directory service are left for the decision of the service provider. Selected attribute types provided by the directory system specification, Recommendation X.520, are:

a) *System attribute types*
   - Aliased object name
   - Knowledge information
   - Object class

b) *Labelling attribute types*
   - Common name
   - Serial number
   - Surname

c) *Geographical attribute types*
   - Country name
   - Locality name
   - State or province name
   - Street address

d) *Organizational attribute types*
   - Organization name
   - Organizational unit name
   - Title

e) *Explanatory attribute types*
   - Business category
   - Description
   - Search guide

f) *Postal attributes*
   - Physical delivery office name
   - Post office box
   - Postal address
   - Postal code
   - Registered address

g) *Telecommunications addressing attribute types*
   - Destination indicator
   - Facsimile telephone number
   - ISDN address
   - Registered address
   - Telephone number
   - Teletex terminal identifier
   - Telex number
   - X.121 address

h) *Preferences attribute types*
   - Preferred delivery method

i) *OSI application attribute types*
   - Presentation address
   - Supported application context

j) *Relational attribute types*
   - Member
   - Owner
   - Role occupant
   - See also

k) *Security attribute types*
   - User password
   - User certificate
   - Authority revocation list
   - Certificate revocation list
   - CA certificate

Note 1 – Other attribute types may be defined for local scope or on bilateral agreement.

Note 2 – The definition of additional selected attribute types for public directory services is for further study.

Note 3 – Messaging handling, in X.402, defined additional attribute types for MHS specific use (see Annex F).

ANNEX E

(to Recommendation F.500)

MHS selected object classes

See Recommendation X.402 for further details.

Selected object classes provided by the directory systems for MHS depend on the scope of the public directory service chosen by the service provider. It is assumed that the presently defined selected MHS object classes will allow the provision of a useful directory service that intercommunicates well with MHS as defined in X.400-series of Recommendations.

MHS object classes

- MHS (Generic MHS user information)
- MHS organizational user
- MHS distribution list
- MHS message store
- MHS message transfer agent
- MHS user agent

ANNEX F

(to Recommendation F.500)

MHS selected attribute types

It is assumed that the presently defined attribute types defined in X.400-series of Recommendations will provide a useful directory service for message handling systems. The implementation of the attribute types used in the public directory service are left for the decision of the service provider. MHS selected attribute types provided by the X.400 system specification, Recommendation X.402, are:

MHS attribute types

- MHS deliverable content length
- MHS deliverable content types
- MHS deliverable encoded information types
- MHS distribution list members
- MHS distribution list submit permissions
- MHS message store
- MHS O/R addresses
- MHS preferred delivery methods
- MHS supported automatic actions
- MHS supported content types
- MHS supported optional attributes

ANNEX G

(to Recommendation F.500)

User visibility of the search operation

Some examples of filters are shown for the practical use.

G.1 *Possible examples*

ORG = Organization name

OUN = Organizational unit name

G.1.1 *Sales units of TTT or marketing units of TNT*

[(ORG = "TTT"), AND, (OUN = "SALES")] OR [(ORG = "TNT") AND, (OUN ="MARKETING")]

G.1.2 *Marketing or sales units of TTT*

(ORG = "TTT"), AND, [(OUN = "MARKETING, OR OUN = "SALES")]

G.1.3 *All departments of TTT except Marketing*

[(ORG = "TTT"), AND, (OBJECT CLASS = OUN)], AND NOT, [(OUN = "MARKETING")] OR [(OUN = MARK*)]

G.1.4 *All organizations in a country whose telex numbers are in the range of 5030 to 5067*

(OBJECT CLASS = ORG)AND, [(TLX ⩽ 5067), AND, (TLX > 5030)]

G.2 *Practical use and effect of filters*

G.2.1 *Task*

"Retrieve" in the USA, the location (state or province), the telefax number, and voice telephone number for the sales departments of TTT or the marketing departments of TNT. The total elapsed time for retrieving the information should not exceed 10 minutes (600 s) and the maximum number of objects found should not exceed 20.

G.2.2 *Solution/action*

Action

SEARCH

Criteria: Base object: "CTN = USA".

subset: "whole subtree"

Filter

[(TYPE = 3), AND, (ORG = "TTT", AND, OUN = "SALES")
, OR, (ORG = "TNT", AND, OUN = "MARKETING")]

Service controls: {
time limit = 600,
size limit = 20,
priority = medium }

Selection: {
FAX,
TEL,
STN }

Result

The directory will return the requested information within the limits designated by the requestor. If the limits are exceeded, an error indicating the limit that was exceeded and arbitrary collection of partial results are displayed in this example.

ANNEX H

(to Recommendation F.500)

Glossary of terms

Note – Some of the terms included are quoted from X.500-series of Recommendations and are only included to enhance understanding of system related descriptions. Some of the text provided are definitions and others are of explanatory nature. A separate Blue Book named "Definitions" may be used as a further source.

H.1 **abandon**

A directory operation to terminate a request. This operation is not guaranteed outside of the local scope.

Note – This directory system operation is considered to be an optional user facility in the service context.

H.2 **access control**

Method of controlling access to information held in the directory either for retrieval, managing or updating purposes.

H.3 **ADD**

A directory operation to add an object entry or an alias entry to the directory information tree (DIT).

Note – This directory system operation is considered to be an optional user facility in the service context.

H.4 **additional service controls**

Function of a directory system to control certain additional performance criteria.

Note – These service controls are considered to belong to additional optional user facilities.

H.5 **administration**

Denotes a public telecommunications Administration or Recognized Private Operating Agency (RPOA).

H.6 **administration directory management domain (ADMD)**

A DMD which is managed by an Administration or RPOA.

H.7 **alias (entry)**

An entry of the class "alias" containing information used to provide an alternate name for an object. It *points* to the entry that actually contains the information.

H.8 **alias name**

A name for an object where at least one of whose relative distinguished names (RDNs) is that of an alias entry.

H.9 **attribute**

The information of a particular type concerning an object and appearing in an entry describing that object in the directory information base (DIB).

Note – See X.500-series of Recommendations for further details.

H.10 **attribute type**

That component of an attribute which indicates the nature of information given by that attribute.

H.11 **attribute value**

A particular instance of information indicated by an attribute type.

H.12 **attribute value assertion**

A proposition, which may be true, false, or undefined, concerning the values (or perhaps only the distinguished values) of an entry.

H.13 **authentication**

Method to establish security services by means of simple or strong authentication. There are two kinds of authentication: data origin authentication and peer entity authentication.

Note – See Recommendation X.509 for more information.

H.14 **authentication mechanisms**

Authentication mechanisms are used to provide for encryption, data integrity and digital integrity.

H.15 **business category**

Attribute type which specifies the commercial activity of some common objects, e.g. people.

H.16 **chaining**

A feature used by the directory system to communicate between directory system agents (DSAs) to satisfy the users request. To achieve this multiple DSAs must be able to intercommunicate as peers. This feature may be inhibited by the user or service provider through service control parameters that are supplied with the user's request.

Note – A set of agreements is required between the domains (DSAs) wanting to interact based on this method.

H.17 **classified information**

In the context of the directory, directories presently known as "white pages", "yellow pages", etc.

H.18 **common name**

In the context of directory systems:

An attribute type identifying an object that is named. It is the name by which the object is commonly named, and conforms to the naming conventions of the country or culture with which the object is associated.

In the context of message handling systems:

Standard attribute identifying a user or distribution list relative to the entity denoted by another attribute (e.g., an organization name). (See Recommendation X.402.)

H.19 **compare**

An operation of the directory system to compare a value (which is supplied as an argument of the request) with the value(s) of a particular attribute type in a particular object entry.

Note – This directory system operation is considered to be an optional user facility in the service context.

H.20 **copy information**

Replicated information.

H.21 **country name**

An attribute type that identifies a country. A country name is a unique designation of a country. When used as a component of a directory name, it identifies the country in which the named object is physically located or with which it is associated in some other important way. In the context of directory systems a value from ISO 3166 (Alpha-2 country codes) is used.

H.22 **description**

An attribute type which describes the associated object, e.g. as an "Yellow pages" entries.

H.23 **destination indicator** (public telegram)

An attribute type specifying the country and city associated with the object (the addresses) needed to provide the public telegram service.

Note – See CCITT Recommendations F.1 and F.31.

H.24 **directory**

A collection of open systems cooperating to provide directory services.

H.25 **directory entry**

A part of the DIB which contains information about an object.

H.26 **directory information base (DIB)**

The complete set of information to which the directory provides access, and which includes all of the pieces of information which can be read or manipulated using the operations of the directory.

H.27 **directory information tree (DIT)**

The directory information base considered as a tree, whose vertices (other than the root) are the directory entries.

Note – The term DIT is used instead of DIB only in contexts where the tree structure of the information is relevant.

H.28 **directory interrogation**

Methods to get results from a request to a directory by read, compare, list, search or abandon operations.

H.29 **directory management domain (DMD)**

A domain responsible for managing the information contained in a directory and the operation on this information.

H.30 **directory modification**

Methods to change information in a directory by add entry, remove entry, modify entry or modify relative distinguished name functions.

H.31 **directory name**

A construct that singles out a particular object from all other objects. A directory name must be unambiguous (that is, denote just one object). However, it need not to be unique (that is, be the only name which unambiguously denotes the object).

See also *name.*

H.32 **directory schema**

The set of definitions and constraints concerning DIT structure, object class definitions, attribute types and syntaxes which characterize the DIB.

H.33 **directory system agent (DSA)**

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

H.34 **directory user agent (DUA)**

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

H.35 **directory management domain (DMD)**

A collection of one or more DSAs and zero or more DUAs which is managed by a single organization. Management of a DUA by a DMD implies an ongoing responsibility for service to that DUA, e.g. maintenance, or in some cases ownership, by the DMD.

H.36 **distinguished name**

The sequence of relative distinguished names of the entry which represents the object and those of all its subordinate entries (in descending order). Because of the one to one correspondence between objects and object entries, the distinguished name of an object can be considered to also identify the object entry.

H.37 **distinguished value**

An attribute value in an entry which has been designated to appear in the relative distinguished name of the entry.

H.38 **distribution list**

List of O/R addresses for message handling services stored in the directory.

Note – This feature is considered to be an optional user facility in the service context.

H.39 **DIT structure**

The definition for an entry of an object class of the permissible object class or classes to which the immediate superior (or subordinate) may belong and its permissible RDN attribute types.

H.40 **do not dereference alias**

A service control which allows to prohibit that any alias used to identify the entry effected by an operation is to be dereferenced.

See also *alias.*

H.41 **do not use copy**

A service control allowing for prohibition of copied information.

H.42 **entry (directory entry)**

A part of the DIB which describes a particular object, and which consists of information that the directory holds about that object.

H.43 **error code**

Information provided from the directory system for the purpose of indicating to the requestor why a request could not be performed sufficiently.

Note – A local directory domain may transfer the information to the requestor in a way appropriate to local requirements. Error codes may refer to service error, attribute error, update error, security error, referral error, abandon error or name error. They are transferred to service messages for the user.

H.44 **facsimile telephone number**

An attribute type which specifies a telephone number for a facsimile terminal (and optionally its parameters) associated with an object.

H.45 **filter**

A filter parameter applies a test to a particular entry and either is satisfied or not by the entry. The filter is expressed in terms of assertions about the presence or value of certain attributes of the entry, and is satisfied if and only if it evaluates to TRUE.

H.46 **intercommunication**

In the context of directory services a relationship between services, where one of the services is a directory service, enabling the user of a service to communicate with the directory.

Note – The term also applies for the relation between public and private directories, for the relation between directory services of different service providers and for the relation between directory management domains.

H.47 **ISDN address**

An attribute type which specifies an ISDN address associated with an object.

H.48 **knowledge information**

An attribute type which specifies a human-readable accumulated description of knowledge mastered by a specific DSA.

H.49 **locality name**

An attribute type which specifies a locality. When used as a component of a directory name, it identifies a geographical area or locality in which the named object is physically located or with which it is associated in some other important way.

H.50 **list**

An operation in the directory system to obtain a list of immediate subordinates of an explicitly identified entry. Under some circumstances, the list returned may be incomplete.

Note – This directory system operation is considered to be an optional user facility in the service context.

H.51 **local scope**

A service control which restricts the scope of directory operations.

Note – The definition of local scope is itself a local matter, and may, for example, mean a limit within a single DSA or a single DMD.

H.52 **member**

An attribute type which specifies a group of names associated with the object.

H.53 **modify**

An operation in the directory system to perform a series of one or more of the following modifications to a single entry:

- add a new attribute;
- remote an attribute;
- add attribute values;
- remove attribute values;
- replace attribute values;
- modify the RDN of a leaf entry;
- modify alias;
- modify entry.

Note – This directory system operation is considered to be an optional user facility in the service context.

H.54 **modify operations**

These are operations to alter the contents of the directory: add entry, remove entry, modify entry and modify relative distinguished name.

H.55 **multicasting**

This is a special case of distributing simultaneously a request to more than one DSA. See Recommendation X.518.

Note – A set of agreements is required between the domains wanting to interact based on this method.

H.56 **name**

In the context of a directory, the designation of entries and parts thereof. A name must be unambiguous, that is, denote just one object. However, a name need not to be unique, that is be the only name that unambiguously denotes the object.

Note – See X.500-series of Recommendations for further study.

H.57 **naming authority**

An authority responsible for the allocation of names. Each object whose object entry is located at a node in the DIT is, or is closely associated with, a naming authority.

In the context of public directory services, the administration directory management domain administers the part of the DIT covered by entries of that domain. It may act as naming authority for the distinguished names used in the scope of the domain.

H.58 **object (of interest)**

Anything in some "world", generally the world of telecommunications and information processing or some part thereof, which is identifiable (can be named), and which is of interest to hold information on the DIB.

H.59 **object entry**

An entry which is the primary collection of information in the DIB about an object, and which can therefore be said to represent that object in the DIB.

H.60 **object class**

An identified family of objects (or conceivable objects) which share certain characteristics.

Note – See X.500-series of Recommendations for further study.

H.61 **O/R address**

Address of an originator/recipient of messages in the context of message handling.

H.62 **organization name**

An attribute type which specifies an organization. When used as a component of a directory name it identifies an organization with which the named object is affiliated.

H.63 **organization unit name**

An attribute type which specifies an organizational unit. When used as a component of a directory name it identifies an organizational unit with which the named object is affiliated.

H.64 **owner**

In the context of a directory, that attribute type specifying the name of some object which has some responsibility for the associated object.

H.65 **physical delivery office name**

An attribute type which specifies the name of the city, village, etc. where a physical delivery office is situated.

H.66 **post office box**

An attribute type which specifies the post office box by which the object will receive physical delivery. If present, the attribute value is part of the object's postal address.

H.67 **postal address**

An attribute type which specifies the address information required for the physical delivery of postal messages by the postal authority to the named object. Formatted and unformatted postal addresses exist.

Note – See also Recommendations F.401 and X.520.

H.68 **postal code**

An attribute type which specifies the postal code of the named object. If this attribute value is present it will be part of the object's postal address.

H.69 **preferred delivery method**

An attribute type which specifies the object's priority regarding the method to be used for communicating with it.

H.70 **presentation address**

An attribute type which specifies a presentation address associated with an object representing an DSI application entry.

H.71 **priority**

A service control which specifies the priority of a request (low, medium, high) for the service. This is not a guaranteed service in that the directory as a whole does not implement queuing. There is no relationship implied with the use of priorities in underlying layers.

H.72 **private directory management domain (PRDMD)**

A DMD managed by another organization than an Administration.

H.73 **public directory service**

A service provided by Administrations to subscribers and users for the purpose of obtaining information on addresses for telecommunication services and other related information from an electronic directory.

H.74 **read operation**

An operation of the directory system to extract an explicitly identified entry. It may also be used to verify a distinguished name.

Note – This directory system operation is considered to be a basic service feature in the service context.

H.75 **referral**

Request handling by the DSA in the case of failing to find the requested information in the first DSA. In this case the directory may return a referral, which suggests an alternative access point at which the DUA can make its request.

Note 1 – This is an alternative method to chaining or multicasting. The implementation is a local matter.

Note 2 – A set of agreements is requuired between the domains (DSAs) wanting to interact on the basis of this method. Whether referrals are presented to the user or not is a local matter. It has to take into account whether the domain (DSA) being referred to will accept requests from these users.

Note 3 – Referrals to domains (DSAs) without prior agreement (including accounting procedures) with them are undesired.

H.76 **registered address**

An attribute type which specifies a mnemonic for an address associated with an object at a particular city location. The mnemonic is registered in the country in which the city is located and is used in the provision of the public telegram service.

H.77 **relative distinguished name (RDN)**

The unique name of an entry. It consists of a particular sequence of attribute value assertions, each of which is true, concerning the distinguished values of an entry.

H.78 **requestor**

The subscriber, user or system entity making a particular request to the directory.

H.79 **role occupant**

An attribute type which specifies the name of an object that fulfills an organizational role. An attribute value for role occupant is a distinguished name.

H.80 **search guide**

An attribute type which specifies information of suggested search criteria which may be included in some entries expected to be a convenient base-object for the search operation, e.g. country or organization.

H.81 **search operation**

An operation in the directory system to search a portion of the DIT for entries of interest, and to return selected information from those entries.

Note – This directory system operation is considered to be a basic service feature in the service context.

H.82 **security capabilities**

Capabilities of a directory system to provide protection against security threats.

Note 1 – These directory system capabilities are considered to be additional optional user facilities in the service context.

Note 2 – See Recommendation X.509 for explanation of security capabilities.

H.83 **see also**

An attribute type which specifies names of other objects which may be other aspects (in some sense) of the same real-world object.

H.84 **serial number**

An attribute type which specifies an identifier, the serial number of a device.

H.85 **service control**

A function of a directory system to control certain performance criteria. A service control parameter contains the controls, if any, that are to direct the provision of the service.

Note – One service control in the directory system (time limit) is an essential optional user facility. Other specific ones are additional optional user facilities in the service context, if the service provider offers them. See also § 4 of Recommendation F.500.

H.86 **size limit**

A service control which indicates the maximum number of objects to be returned in the results of a search or list operation (the control is only applicable to those operations). If the list size is exceeded, any results equal in number to the size limit should be returned, with the indication that the results are incomplete due to the size limit constraint. If this component is omitted, no maximum is implied.

H.87 **state or province name**

Identifies the geographical subdivision in which the named object is physically located or with which it is associated in some other important way.

H.88 **street address**

An attribute type which specifies a site for the local distribution and physical delivery in a postal address, i.e. the street name, place, avenue and the house number. When used as a component of a directory name, it identifies the street address at which the named object is located or with which it is associated in some other important way.

H.89 **subclass**

Relative subordinate to a superclass, an object class derived from a superclass. The members of the subclass share all the characteristics of another object class (the superclass) and additional characteristics possessed by none of the members of that class (the superclass).

H.90 **subscriber**

A user of a telecommunication service, normally based on a contract with the provider of a public service.

H.91 **superclass**

Relative superior to a subclass, an object class from which a subclass is derived.

H.92 **supported application context**

An attribute type which specifies the object identifier of an application context that the object (an OSI application entity) supports.

H.93 **surname**

An attribute type which specifies the linguistic construct which normally is inherited by an individual from the individual's parent or assumed by marriage, and by which the individual is commonly known.

H.94 **telephone number**

An attribute type which specifies a telephone number associated with an object.

Note – The format of internationally agreed telephone numbers follows Recommendation E.164.

H.95 **teletex terminal identifier**

An attributed type which specifies the teletex terminal identifier for a teletex terminal associated with an object.

Note – The format follows Recommendation F.200.

H.96 **telex answer-back**

An attribute type which specifies the telex terminal identifier for a telex terminal associated with an object.

Note – The format follows Recommendation F.60.

H.97 **telex number**

An attribute type which specifies the telex number, country code, and answer-back code of an telex terminal.

Note – The format follows Recommendation F.69.

H.98 **time limit**

A service control that indicates the maximum elapsed time, in seconds, within which the service should be provided. If the constraint connot be met, an error is reported, unless it was a search or a list operation, in which case partial results should be returned to the DUA with the indication that a time limit problem has been encountered. If this component is omitted, no time limit is implied.

Note – This service control is an essential optional user facility.

H.99 **title**

An attribute type which specifies the designated position or function of the object within an organization.

H.100 **user**

In telecommunication service context: A human being using a service.

In a technical context: A human being, an entity or a process.

Note – A user will not necessarily be a subscriber of a telecommunication service.

H.101 **user certificate**

See Recommendations X.520 and X.509.

H.102 **wildcard**

In the context of directory services, a way to replace unknown parts of attributes for a request to the directory.

H.103 **user password**

A sequence of characters to identify a user.

H.104 **videotex user number**

An attribute type which specifies a videotex user number associated with an object.

H.105 **white pages**

See under "classified information".

H.106 **X.121 address**

An attribute type which specifies a number from the X.121 numbering plan associated with an object.

H.107 **yellow pages**

See under "classified information".

ISBN 92-61-03301-6