EUR AMHS Manual

Appendix A

Abbreviations, Glossary and Definitions	
Document Reference:	EUR AMHS Manual, Appendix A
Author:	ICAO AFSG PG
Revision Number:	Version 6.0
Date:	14/04/11
Filename:	EUR_AMHS_Manual-Appx_A-v6_0.doc

Document Control Log

Edition	Date	Comments	section/pages affected
0.1	29/07/2005	Created from draft EUR AMHS Manual, version 0.5, Appendix A, B and C.	all
0.2	15/08/2005	Updated by abbreviations used in the EUR AMHS Profile and Conformance Test documents	chapter 1
0.3	28/09/2005	Insert of additional abbreviations	chapter 1
0.4	28/01/2006	Insert of additional abbreviations and definitions	chapter 1 and 2
0.5	08/03/2006	Reformatting (*Notes*)	all
0.6	19/03/2006	Insert of additional abbreviations	chapter 1
1.0	27/04/2006	Adopted version (AFSG/9)	
1.1	11/01/2007	Insert of abbreviations from Manual update of Main Part and Appendices	chapter 1
2.0	26/04/2007	Adopted version (AFSG/10)	
3.0	24/04/2008	Adopted version (AFSG/11) – without changes	
3.1	17/11/2008	Change of references from ICAO Doc 9705 to ICAO Doc 9880 (CP-AMHSM-08-006), editorial improvements	References, Chapter 2 Note
3.2	13/02/2009	Incorporation of CP-AMHSM-08-007	Chapter 2 - ***Indirect AMHS user***
3.3	11/03/2009	Update of the referenced documents	References
4.0	02/04/2009	Adopted version (AFSG/12)	
5.0	17/06/2010	Adopted version (AFSG/14) – without changes	
5.1	24/09/2010	Incorporation of CP-AMHSM-10-001, minor editorial updates	References
5.2	30/11/2010	Remark concerning Doc 9739 (CAMAL) added	References
6.0	14/04/2011	Adopted version (AFSG/15)	

Table of contents

References

ICAO Documentation

[1] Aeronautical Telecommunications, Annex 10, Volume III, Part I, Chapter 3

[2] ICAO Doc 9880-AN/466: Manual on Detailed Technical Specifications for the Aeronautical Telecommunication Network (ATN) using ISO/OSI Standards and Protocols, Part II – Ground-Ground Applications - Air Traffic Services Message Handling Services (ATSMHS), First Edition – 2010

[3] ICAO Doc 9739, Comprehensive ATN Manual (CAMAL), Part 1, Section 5.1 Abbreviations (not further maintained by ICAO)

[4] ICAO Doc 9739, Comprehensive ATN Manual (CAMAL), Part 1, Section 5.2 Definitions (not further maintained by ICAO)

[5] ICAO Doc 9739, Comprehensive ATN Manual (CAMAL), Part 1, Section 5.3 ATNP Lexicon (not further maintained by ICAO)

General technical literature

[6] ISO/IEC 10021-2: Information Technology – Message Handling Systems (MHS): Overall architecture

1. Abbreviations

(Taken from the ICAO Doc 9739, Comprehensive ATN Manual (CAMAL), Part 1, Section 5.1 Abbreviation, which was not further maintained by ICAO, and several terms are added by AFSG Planning Group)

A

A	Administration domain name (X.400)
AAC	Aeronautical administrative communications
ACARS	Aircraft communication addressing and reporting system
ACC	Air Traffic Control Centre
ACCESS	ATN Compliant Communications European Strategy Study
ACK	Acknowledgement
ACP	Aeronautical Communications Panel (ICAO)
ACSE	Application control service element
Ad	Destination Address (CIDIN)
AD	Administrative domain
ADI	Administrative domain identifier
ADM	Administrative identifier
ADMD	Administrative management domain
ADS	Address (AFTN procedure signal)
ADS	Automatic dependent surveillance
Ae	Entry Address (CIDIN)
AE	Application Entity
AES	Aircraft earth station
AFI	Authority and format identifier
AFS	Aeronautical fixed service
AFSG	Aeronautical fixed service Group (ICAO EANPG)
AFTN	Aeronautical fixed telecommunication network
AI	Aircraft identifier
AIDC	ATS inter-facility data communication
AINSC	Aeronautical industry services communication
AIRAC	Aeronautical Information, Regulation and Control
AIS	Aeronautical information services
AMC	ATS Messaging Management Centre
AMH	Application (profile) Message Handling
AMHS	ATS message handling system
AMS	Aeronautical mobile service
AMSS	Aeronautical mobile satellite service
ANM	ATFM notification messages
ANSP	Air Navigation Service Provider
AOC	Aeronautical operational control
AOP	ATN OSI profile
AP	Application process
APC	Aeronautical passenger communications
APRL	ATN protocol requirements list
ARS	Administrative region selector
ASN.1	Abstract syntax notation one
ASO	Application service object
ATC	Air traffic control
ATCC	Air traffic control centre
ATFM	Air traffic flow management
ATIS	Automatic terminal information service
ATM	Air traffic management
ATN	Aeronautical telecommunication network
ATNP	Aeronautical telecommunication network panel
ATS	Air traffic services
ATSC	Air traffic services communication
ATSMHS	ATS message handling services
ATSU	Air traffic service unit
AU	Access unit
Ax	Exit Address (CIDIN)

B

Bas	Basic ATS Message Handling Service (as used in Appendix B)
BCD	Binary coded decimal
BIS	Boundary intermediate system
BER	Basic Encoding Rules

C

C	Country name (X.400)
CAA	Civil aviation authority
CAAS	Common AMHS Addressing Scheme
CCC	Co-operating COM Centre
CCITT	International telegraph and telephone consultative committee (now ITU-T)
CIDIN	Common ICAO data interchange network
CL	Connectionless
CLNP	Connectionless-mode network protocol
CM	Context management
CMA	Context management application
CMC	CIDIN Management Centre
CN	Common name (X.400)
CNS	Communications, navigation and surveillance
CO	Connection oriented
COM	Communication
COP	Character oriented protocol
COTS	Commercial Off The Shelf
CPDLC	Controller-pilot data link communications
CTD	CIDIN Test Driver

D

DCE	Data communications equipment
DIT	Directory information tree
DL	Distribution list
DLAC	Data link application coding
DNIC	Data network identification code
DR	Delivery Report
DR	Disconnect request
DSA	Directory system agent
DSP	Domain specific part
DTE	Data terminal equipment
DUA	Directory user agent

E

EANPG	European Air Navigation Planning Group (ICAO)
ECAC	European Civil Aviation Conference
ECDSA	Elliptic Curves Digital Signature Algorithm
ECG	EATMP Communication Gateway
EIT	Encoded Information Type
ES	End system
EUR	ICAO Region Europe
Ext	Extended ATS Message Handling Service (as used in Appendix B)

F

FANS	Future air navigation system
FDDI	Fibre distributed data interface
FG	Functional group
FIB	Forwarding information base
FIR	Flight information region
FIRST	First multipartite International Realisation of ICAO SARPs AMHS Trials
FIS	Flight information services
FMS	Flight management system
FP	Flight plan
FPL	Flight plan

G

GA	General aviation
GES	Ground earth station

H

HDLC	High-level data link control
HF	High frequency
HMI	Human machine interface

I

IA5	International Alphabet No. 5
IACSP	International aeronautical communication service provider
IATA	International Air Transport Association
ICAO	International Civil Aviation Organisation
ICC	Inter-centre co-ordination
ICD	International code designator
ID	Identification
IDI	Initial domain identifier
IDP	Initial domain part
IDRP	Inter-domain routing protocol
IEC	International electro technical commission
IFR	Instrument flight rules
IP	Internet protocol
iPAX	Internet protocol for ATS data exchange
IPM	Interpersonal messaging
IPMS	Interpersonal Messaging System
IPN	Interpersonal Notification
IPS	Internet Protocol Suite
IPv4	Internet protocol version 4

IPv6	Internet protocol version 6
IS	Intermediate system
ISDN	Integrated services digital network
ISO	International organisation for standardisation
ISOPA	ISO protocol architecture
ISP	International standardised profile
ITU-T	International Telecommunication Union — Telecommunication Standardisation Sector
IPM	Inter-Personal Message
IPN	Interpersonal Notification
IUT	Implementation Under Test

L

LAN	Local area network
LLC	Logical Link Control
LOC	Location identifier

M

MAC	Medium Access Control
MD	Management domain
MF	MHS-form (address)
MH	Message Handling
MHE	Message Handling Environment
MHS	Message handling services
MHS	Message handling system
MIB	Management Information Base
MODE S	Mode select
MORTs	Managed objects requirement templates
MS	Message store
MS (94)	Message Store ‘94
MT	Message transfer
MTCU	Message transfer and control unit
MTA	Message transfer agent
MTD	MTA Test Driver
MTE	Message Transfer Envelope
MTP	Manual teletypewriter procedures
MTS	Message Transfer Service
MTS	Message transfer system

N

NDR	Non-Delivery Report
NET	Network entity title
NOTAM	Notice to airmen
NPDU	Network protocol data unit
NRN	No-Receipt Notification
NSAP	Network service access point
NTN	Network terminal number
N-SEL	Network selector

O

O	Organisation name (X.400)
OG	Operations Group (AFSG)
OID	Object identifier
OPMET	Operational meteorological traffic
O/R	Originator/recipient
OSI	Open system interconnection
OU	Organisational unit name (X.400)

P

P1	Message Transfer Protocol
P2	Inter-Personal Messaging Content Type
P3	Message Submission and Delivery Protocol
P7	Message Retrieval Protocol
PANS-RAC	Procedures for Air Navigation Services — Rules of the Air and Air Traffic Services
PCI	Protocol control information
PDAI	Predetermined distribution addressee indicator
PDR	Potential Defect Report
PDU	Protocol data unit
PENS	Pan-European Network Services
PER	Packed encoding rules
PG	Planning Group (AFSG)
PIB	Policy information base
PICS	Protocol Implementation Conformance Statement
PIREP	Pilot reports
PN	Personal name (X.400)
PRL	Profile Requirements List
PRMD	Private management domain
PSAP	Presentation service access point
PSDN	Packet switched data network
PSEL	Presentation selector
PTT	Post, telephone and telegraph
PVC	Permanent virtual circuit

Q

QoS	Quality of service
QTA	AFTN procedure signal

R

RD	Routing domain
RDC	Routing domain confederation
RDF	Routing domain format

RDI	Routing domain identifier
RDN	Relative distinguished name
RFC	Request For Call
RIB	Routing information base
RN	Receipt Notification
RPT	Repeat (AFTN procedure signal)
RTE	Report Transfer Envelope

S

SAR	Search and rescue
SARPs	Standards and recommended practices
SEL	Selector
SICASP	SSR Improvements and Collision Avoidance Systems Panel
SIGMET	Significant meteorological information
SLA	Service level agreement
SN	Subnetwork
SNPA	Subnetwork point of attachment
SPACE	Study and Planning of AMHS Communications in Europe
S-SEL	Session selector
SSAP	Session service access protocol
SSR	Secondary surveillance radar
SUT	System under test
SVC	Switched Virtual Connection
SYS	System identifier

T

TBD	To be defined
TCP/IP	Transmission control protocol/internet protocol
TP	Transport Protocol
TSAP	Transport service access point
TSEL	Transport selector

U

UA	User agent
UHF	Ultra high frequency

V

VDL	Very high frequency digital link
VER	Version identifier
VHF	Very high frequency

W

WAN	Wide area network

X

XF	Translated-form (address)
XMIB	ATN Cross-Domain Management Information Base

2. Glossary and Definitions

Note. – This glossary of terms has been compiled using ITU-T X.400 recommendation (1997), ISO/IEC 10021-2 [6]and ICAO AMHS technical specifications [2] and the Comprehensive ATN Manual (Definitions [4] and ATNP Lexicon [5]). In case of notable differences in definitions from various sources, all are presented. The source is denoted by [ITU-T], [ISO] and [SARPs] where appropriate.

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

In the context of message handling services, the unit which enables users of one service to intercommunicate with message handling services, such as the IPM service. [ITU-T]

Actual recipient In the context of message handling, a potential recipient for which delivery or affirmation takes place. [ITU-T]

Address domain A set of address formats and values administered by a single address authority. Under the ISO plan, any address authority may define subdomains within its own domain and delegate authority within those subdomains. [4]

Addressing authority Defines formats and/or values of NSAP addresses within its jurisdiction. [4]

Addressing (logical) Logical addressing means that the address defined in the addressing plan and used to locate the addressed object is a virtual address which is a substitute of the actual (physical) address of an object. Address mapping functions have to fulfil this substitution, carefully maintaining unambiguity of identification of objects. [5]

Addressing (physical) Physical addressing means that the address defined in the addressing plan and used to locate the addressed object is the physical, i.e. hardwired, hard-coded or configured address of the object. An example of a physical address is the ICAO 24-bit aircraft address used for the SSR Mode S transponder. [5]

Administration In the context of ITU-T, an Administration (member of ITU) or a Recognised Operating Agency (ROA). [ITU-T]

Administrative domain A collection of end systems, intermediate systems and subnetworks operated by a single organisation or administrative authority. An administrative domain may be internally divided into one or more routing domains. [4]

Administration domain name (A) 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. [ITU-T]

An administration-domain-name is a standard attribute that identifies an ADMD relative to the country denoted by a country-name. The value of an administration-domain-name is a Printable String chosen from a set of such strings that is administered for this purpose by the country alluded to above.

Note. – In the context of ATSMHS, the administration-domain-name assigned to ICAO by ITU-T is A = "ICAO". [ISO]

Administration management domain (ADMD) A management domain that comprises messaging systems managed (operated) by a service provider. [ITU-T]

A management domain that comprises systems managed (operated) by a service provider. [ISO]

Aeronautical administrative communications (AAC) Communications used by aeronautical operating agencies related to the business aspects of operating their flights and transport services. These communications are used for a variety of purposes, such as flight and ground transportation bookings, deployment of crew and aircraft, or any other logistic purposes that maintains or enhances the efficiency of overall flight operation. [4]

Aeronautical mobile satellite service (AMSS) Provides packet-mode data and circuit-mode data and voice service to aircraft and ground users provided by a satellite subnetwork which comprises satellites, Aircraft Earth Stations (AESs), Ground Earth Stations (GESs) and associated ground facilities such as a network co-ordination centre. [4]

Aeronautical operational control (AOC) Communication required for the exercise of authority over the initiation, continuation, diversion or termination of flight for safety, regularity and efficiency reasons. [4]

Aeronautical passenger communications (APC) Communications relating to the non-safety voice and data services to passengers and crew members for personal communications. [4]

Aeronautical telecommunication network (ATN) An internetwork architecture which allows ground, air-to-ground and avionics data subnetworks to interoperate by adopting common interface services and protocols based on the International Organisation for Standardisation (ISO) Open Systems Interconnection (OSI) reference model. [4]

AF-address The AF-address (AFTN-form address) is either an AFTN addressee indicator as specified in Annex 10, Volume II, paragraph 4.4, which is used to locate AMHS users, either direct or indirect, in the AFTN address space or a predetermined distribution addressee indicator (PDAI) as specified in Annex 10, Volume II, paragraph 4.4.14. [SARPs]

Air traffic control (ATC) A service operated by an appropriate authority to promote the safe, orderly and expeditious flow of air traffic. [4]

Air traffic services communications (ATSC) Communications related to air traffic services including air traffic control, aeronautical and meteorological information, position reporting and services related to safety and regularity of flight. This communication must involve one or more air traffic service administrations. This term is used for purposes of address administration. [4]

Alternate recipient In the context of message handling, a user or a distribution list to which a message or probe may be conveyed if, and only if, it cannot be conveyed to a particular preferred recipient. The Alternate Recipient may be specified by the originator, by the recipient , or by the recipient MD. [ITU-T]

Application Software providing services to its users as a consistent set of functionality; e.g. the ATC related functions implemented in the server(s) and/or controller work position host computers. [4]

Application entity (AE) Part of an application process that is concerned with communications within the OSI environment. The aspects of an application process that need to be taken into account for the purposes of OSI are represented by one or more AEs. [4]

Application process (AP) A set of resources, including processing resources, within a real open system which may be used to perform a particular information processing activity. [4]

Application service The abstract interface between the (N)-service and the (N)-service user, where N refers to the application layer; thus it is the boundary between the ATN-App-AE and the application-user. [4]

ATN applications Refers to applications that support ATM or aeronautical industry functions and that are designed to operate across an OSI communications system. ATN applications are always distributed applications, i.e. peer processes are hosted by different end systems which are interconnected. [4]

ATN communication services The ATN communication services are provided to ATN users that require ground-ground or air-ground data communication. The ATN accommodates different grades of services which can be expressed by quality of service parameters and by communication priorities. [5]

ATN environment The term relates to functional and operational aspects around the ATN as a complete end-to-end communication system. [4]

ATN internet (ATNI) An implementation of the ISO OSI network layer services and protocols for support of interprocess data communication between aeronautical host computers. It is defined to be the collection of the connected internetwork routers and subnetworks that conform to ATN internetwork requirements. [4]

ATN network operating concept An ATN network operating concept will address the administrative, operational, institutional and policy issues and additional (non-SARPs) technical aspects to enable the efficient and correct operation of the ATN. [4]

ATN router The communication element that manages the relaying and routing of data while in transit from an originating ATN host computer to a destination ATN host computer. In ISO terms, an ATN router comprises an OSI intermediate system and an end system supporting a systems management agent. [4]

ATN routing domain confederation (RDC) The ATN RDC is the set of interconnected routing domains that together form the ATN internetwork. [4]

ATN services The ATN services are provided to ATN users that require ground-ground or air-ground data communication. The ATN internet service is provided at the transport layer (service access point). The ATN accommodates different grades of services which can be expressed by Quality of Service parameters. [4]

ATN system applications System applications support the operation of the ATN communication services and are either not directly or not at all used by ATN users but rather by the service providers, operators or other ATN applications. Typical examples of ATN system applications are the ATN directory service, ATN context management or ATN systems management. [5]

ATN systems management The ATN Systems Management provides mechanisms for monitoring, control and co-ordination of resources necessary to provide ATN services. ATN systems management is based on OSI system management principles and may be distributed, centralised or local. [4]

ATS message handling services (ATSMHS) Procedures used to exchange ATS messages over the ATN such that the conveyance of an ATS message is in general not correlated with the conveyance of another ATS message by the service provider. There are two ATS message handling services. They are the ATS message service and the ATN pass-through service. [4]

ATS Message Handling Services (ATSMHS) or ATS message service Both terms apply to the application or functional service delivered to service users in compliance with the technical provisions for the ATN (i.e. ref. [1], sub-volume III).

Two levels of service are defined within the ATS Message Service:

i) the Basic ATS Message Service; and

ii) the Extended ATS Message Service.

Both levels of service are compatible with one another. The Extended ATS Message Service is functionally a superset of the Basic ATS Message Service, and it is backward compatible with the Basic ATS Message Service. [SARPs]

ATS message-handling system (AMHS) Term used to technically identify the set of systems providing the ATS message service. [SARPs]

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

It describes a user or DL and may also locate it in relation to the physical or organisational structure of the MHS (or the network underlying it).

An attribute has the following parts:

a) attribute type (or type) that denotes a class of information;

b) attribute value (or value) that is an instance of the class of information the attribute type denotes.

Attributes are of the following two kinds:

a) standard attribute: an attribute whose type is bound to a class of information by the ISO/IEC 10021-2 specification;

b) domain-defined attribute: an attribute whose type is bound to a class of information by a Management Domain (MD). [ISO]

Attribute list In the context of message handling, a data structure, an ordered set of attributes, that constitutes an O/R address. [ITU-T]

Attribute type An identifier that denotes a class of information (e.g. personal names). It is a part of an attribute. [ITU-T]

Attribute value An instance of the class of information an attribute type denotes (e.g. a particular personal name). It is a part of an attribute. [ITU-T]

Automatic dependent surveillance (ADS) A technique in which aircraft automatically provide, via a data link, data derived from on-board navigation and position-fixing systems, including aircraft identification, four-dimensional position and additional data as appropriate. ADS is a data link application. [4]

Basic service In the context of message handling, the sum of features inherent in a service. [ITU-T]

Basic ATS message service The Basic ATS Message Service is based on the first version of the ISO/IEC ISPs, published in 1994 and based on the ISO/IEC 10021:1990 set of standards. [SARPs]

Body Component of the content of a message. Another component is the heading. [ITU-T]

Body part Component of the body of a message. [ITU-T]

Boundary intermediate system (BIS) An intermediate system that is able to relay data between two separate routing or administrative domains. [4]

Character set Standard attribute values and domain-defined attribute types and values are constructed from Printable Strings [SARPs]

Common name (CN) 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 organisational name). [ITU-T]

A common-name is a standard attribute that identifies a user or DL relative to the entity denoted by another attribute (e.g. an organisation-name). The value of a common-name is a Printable String. The string is chosen from a set of such strings that is administered for this purpose (and perhaps others) by the entity alluded to above. [ISO]

Congestion In the ATN internet sense, congestion describes the state where the network is overloaded. Typical effects of congestion are extended transit delays, drastically reduced throughput and the loss of data packets. [5]

Congestion avoidance Techniques that regulate the data flow into the network in order to prevent the network from getting overloaded. These encompass both open-loop techniques, which ensure that a traffic contract specified by the source is respected, and closed-loop techniques, which monitor signals generated by the network and adapt the traffic generated by the sources accordingly. [5]

Congestion management This term refers to a set of rules and techniques which prevent congestion, e.g. by monitoring actual network load. Co-operative interaction of *all* end systems is required in order to prevent individual end-systems taking up the throughput saved by well behaving systems. [5]

Congestion recovery/congestion control This term refers to a mechanism which reacts to congestion after it has occurred in order to remove the overload condition. Congestion recovery can be initiated only after congestion has been experienced and is not able to safely prevent congestion in the network. [5]

Conformance test A test of a protocol implementation with respect to its specifications.

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

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

Context management (CM) Refers to an ATN application. This application implements an ATN logon service allowing initial aircraft introduction into the ATN. The logon service also allows indication of all other data link applications on the aircraft. CM also includes functionality to forward addresses between ATC centres. Thus, CM is a logon and simple directory service. [4]

Note. – "Context management" is a recognised OSI presentation layer term. The OSI use and the ATN use have nothing in common.

Conversion In the context of message handling, a transmittal event in which an MTA transforms parts of a message's content from one encoded information type to another, or alters a probe so it appears that the described messages were so modified. [ITU-T]

Country name (C) 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. [ITU-T]

A country-name is a standard attribute that identifies a country. The value of a country-name is a Printable String that gives the character pair assigned to the country by ISO 3166.

Note. – In the context of ATSMHS, the country-name assigned to ICAO by ITU-T is C = "XX" [ISO]

Delivery In the context of message handling, a transmittal step in which an MTA conveys a message or report to the MS, UA or AU of a potential recipient of the message or of the originator of the report's subject message or probe. [ITU-T]

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

Direct AMHS user An ATS Message Service user who engages in the ATS Message Service at an ATS Message User Agent. A direct AMHS user may belong to two subgroups as follows:

1) human users who interact with the ATS Message Service by means of an ATS Message User Agent connected to an ATS Message Server; and
2) host users which are computer applications running on ATN end systems and interacting with the ATS Message Service by means of application programme interfaces. [SARPs]

Direct submission In the context of message handling, a transmittal step in which the originator's UA or MS conveys a message or probe to an MTA. [ITU-T]

Directory A collection of open systems co-operating to provide directory services. [ITU-T]

Directory name 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. [ITU-T]

When locally supported, a Directory name identifies an object to the Directory. By presenting such a name to the Directory, the MHS can access a user's or DL's Directory entry and from that entry the Message Transfer System (MTS) can obtain the user's or DL's OR-address. [ISO]

Directory service The ATN directory service provides the ATN user with the addressing information which is associated with the application process title or application entity title used as input to the directory. The addressing information provided by the directory service includes the network address as well as further technical addresses on the layers above, as required or applicable. Furthermore, the ATN directory service resolves generic application process titles or application entity titles, i.e. names which may be incomplete or contain "don't care" elements, into the corresponding (list of) non-generic application process titles or application entity titles. [5]

Directory system agent (DSA) An OSI application process which is part of the directory, and whose role is to provide access to the directory information base to DUAs and/or other DSAs. [ITU-T]

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 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. [ITU-T]

Direct user In the context of message handling, a user that engages in message handling by direct use of the MTS. [ITU-T]

Distribution list (DL) In the context of message handling, the functional object, a component of the message handling environment, that represents a pre-specified group of users and other distribution lists and that is a potential destination for the information objects an MHS conveys. Membership can contain O/R names identifying either users or other distribution lists. [ITU-T]

Distribution list expansion In the context of message handling, a transmittal event in which an MTA resolves a distribution list, among a message's immediate recipients, to its members. [ITU-T]

Distribution list name An O/R name allocated to represent a collection of O/R addresses and directory names. [ITU-T]

Domain See management domain. [ITU-T]

Domain A set of end systems and intermediate systems that operate according to the same routing procedures and that is wholly contained within a single administrative domain. [4]

Domain-defined attributes Optional attributes of an O/R address allocated to names in the responsibility of a management domain. [ITU-T]

Element of service A functional unit for the purpose of segmenting and describing message handling features. [ITU-T]

Encoded information type (EIT) 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. T.51 text, group 3 facsimile) on an individual portion of the content. [ITU-T]

End system (ES) A system that contains the seven OSI layers and contains one or more end user application processes. [4]

Engineering trials In contrast to operational trials, engineering trials may be based on pre-operational, prototype or experimental equipment. Aim is to demonstrate the technical feasibility and correctness of applied techniques, concepts and specifications. [5]

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

Explicit conversion In the context of message handling, a conversion in which the originator selects both the initial and final encoded information types. [ITU-T]

Extended ATS message service The Extended ATS Message Service is based on the third version of the ISO/IEC ISPs, published in 1999 and based on the ISO/IEC 10021:1999 set of standards. [SARPs]

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

Functional requirements Operational requirements that determine what function a system should perform. They can usually be expressed by a verb applying to a type of data, e.g. display aircraft position. [4]

Gateway A system used to interconnect dissimilar networks. A gateway may contain all seven layers of the OSI reference model. [4]

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

Heading A component of an IP-message. Other components are the envelope and the body. [ITU-T]

Immediate recipient In the context of message handling, one of the potential recipients assigned to a particular instance of a message or probe (e.g. an instance created by splitting). [ITU-T]

Implementation under test Implementation of one or more protocols, which are to be studied by testing

Implicit conversion In the context of message handling, a conversion in which the MTA selects both the initial and final encoded information types. [ITU-T]

Indirect AMHS user An ATS Message Handling Service user at an AFTN station, using an AFTN/AMHS Gateway to communicate with other ATS Message Handling Service users. [SARPs]

Indirect submission In the context of message handling, a transmittal step in which an originator's UA conveys a message or probe to an MTA via an MS. [ITU-T]

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

Note. – Indirect users communicate via access units with direct users of MHS. [ITU-T]

Institutional issues Issues related to ownership, control and responsibility for correct implementation and operation of systems which involve more than one state or organisation. [5]

Integrated services digital network (ISDN) A public telecommunications network that supports the transmission of digitised voice and data traffic on the same transmission links. [4]

Intercommunication In the context of message handling, a relationship between services, where one of the services is a message handling service, enabling the user of the message handling service to communicate with users of other services

Note. Examples are the intercommunication between the IPM service and the telex service, and the intercommunication between message handling services and physical delivery services. [ITU-T]

Intermediate system (IS) A system comprising the lower three layers of the OSI reference model and performing relaying and routing functions. [4]

Internetwork A set of interconnected, logically independent heterogeneous subnetworks. The constituent subnetworks are usually administrated separately and may employ different transmission media. [4]

Interoperability test *A* test of a protocol implementation in a model of a communication network where fault-free interaction with peer implementations can be verified.

Interpersonal messaging service Messaging service between users belonging to the same management domain or to different management domains by means of message handling, based on the message transfer service. [ITU-T]

IP-message The content of a message in the IPM Service. [ITU-T]

Management domain Resources that for systems management purposes are represented by managed objects. A management domain possesses at least the following quantities: a name that uniquely identifies that management domain, identification of a collection of managed objects that are members of the domain, and identification of any inter-domain relationships between this domain and other domains. [4]

Management domain (MD) In the context of message handling, a set of messaging systems – at least one of which contains, or realises, an MTA – that is managed by a single organisation. It is a primary building block used in the organisational construction of MHS. It refers to an organisational area for the provision of services.

Note. – A management domain may or may not necessarily be identical with a geographical area. [ITU-T]

Management domain name A unique designation of a management domain for the purpose of sending and receiving messages. [ITU-T]

Members In the context of message handling, the set of users and distribution lists implied by a distribution list name. [ITU-T]

Message An instance of the primary class of information object conveyed by means of message transfer, and comprising an envelope and content. [ITU-T]

Message handling (MH) A distributed information processing task that integrates the intrinsically related subtasks of message transfer and message storage. [ITU-T]

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

The sum of all components of message handling systems.

Note. – Examples of components are:

- *message transfer agents;*
- *user agents;*
- *message stores;*
- *users.*

[ITU-T]

Message handling service Service provided by the means of message handling systems.

Note 1: Service may be provided through administration management domains or private management domains.

Note 2: Examples of message handling services are:

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

[ITU-T]

Message handling system (MHS) The functional object, a component of the message handling environment, that conveys information objects from one party to another. [ITU-T]

Message storage The automatic storage for later retrieval of information objects conveyed by means of message transfer. It is one aspect of message handling. [ITU-T]

Message store (MS) The functional object, a component of MHS, that provides a single direct user with capabilities for message storage. [ITU-T]

Message transfer (MT) The non-real-time carriage of information objects between parties using computers as intermediaries. It is one aspect of message handling. [ITU-T]

Message transfer agent (MTA) A functional object, a component of the MTS, that actually conveys information objects to users and distribution lists. [ITU-T]

Message transfer service A service that deals with the submission, transfer and delivery of messages for other messaging services. [ITU-T]

Message transfer system (MTS) The functional object consisting of one or more message transfer agents which provides store-and-forward message transfer between user agents, message stores and access units. [ITU-T]

MF-address An MF-address is the OR-address of an AMHS user. [ITU-T]

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

Mnemonic O/R address An O/R address that mnemonically 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. [ITU-T]

A mnemonic OR-address is one that provides a memorable identification for a user or DL. It identifies an ADMD and a user or DL relative to that ADMD. [ISO]

Mobile subnetwork A subnetwork connecting a mobile system with another system not resident in the same mobile platform. These subnetworks tend to use free-radiating media (e.g. radio) rather than "contained" media (e.g. wire); thus they exhibit broadcast capabilities in the truest sense. [4]

Naming authority An authority responsible for the allocation of names.

Note. – In the context of ATSMHS, ICAO is the naming authority, responsible for the allocation of private-domain-name and organisation-name. [ITU-T]

Network address In the context of message handling, a standard attribute of an O/R address form that gives the network address of a terminal. It comprises the numbering digits for network access points from an international numbering plan. [ITU-T]

Network management The set of functions related to the management of various OSI resources and their status across the network layer of the OSI architecture. [4]

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

Non-registered access In the context of message handling services, access to the service through publicly available telecommunications means by users who have neither been explicitly registered by the service provider, nor been allocated an O/R address. [ITU-T]

Operating concept The technical functionality of a system and its inherent capabilities regarded from the system operator's point of view. This includes the interaction between user and system, the services provided by the system as well as the internal operation of the system. [4]

Operational concept Describes, from the user's point of view, the operational requirements, constraints and prerequisites within which a technical system is supposed to work as well as the inherent capabilities of the system. It describes the interaction between the user and the system as well as the services the user may expect from the system. Broad outline of an operational structure able to meet a given set of high level user requirements. It comprises a consistent airspace organisation, general operational procedures and associated operational requirements for system support. [4]

Operational trials Operational trials are based on operational environment. This includes operational systems and operational equipments, e.g. routinely scheduled flights in an operational ATS environment. Aim is to demonstrate the operational acceptance and correctness of applied mechanisms, applications and concepts. [5]

O/R address In the context of message handling, an attribute list that distinguishes one user or DL from another and identifies the user's point of access to MHS or the distribution list's expansion point. [ITU-T]

To convey a message, probe or report to a user, or to expand a DL specified as a potential recipient of a message or probe, the MTS must locate the user or DL relative to its own physical and organisational structures. OR-addresses are the data structures by means of which all such location is accomplished. OR-addresses are constructed from attribute lists. [ISO

O/R address form An OR-address shall only take the mnemonic form. [ITU-T]

Organisational unit name (OU) Standard attribute of an O/R address as a unique designation of an organisational unit of an organisation for the purpose of sending and receiving of messages. [ITU-T]

Organisation-name (O) Standard attribute of an O/R address as a unique designation of an organisation for the purpose of sending and receiving of messages. [ITU-T]

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

An identifier by means of which a user can be designated as the originator, or a user or DL designated as a potential recipient of a message or probe. An OR-name comprises a Directory name, an OR-address, or both. [ISO]

Originator In the context of message handling, the user (but not distribution list) that is the ultimate source of a message or probe. [ITU-T]

Performance requirements Requirements with respect to the performance of a system (e.g. reliability, availability, response time, processing delay, etc.) and are derived from operational requirements. In general, they describe the minimum performance figures that a system must provide in order to fulfil the operationally required functions. [4]

Personal name (PN) 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 organisation name).

Note. – In the context of ATSMHS, the personal-name attribute is not used at present. [ITU-T]

Private domain name (P) 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.
[ITU-T]

A private-domain-name is a standard attribute that identifies a PRMD. As a national matter, this identification may be either relative to the country denoted by a country-name (so that PRMD names are unique within the country), or relative to the ADMD identified by an administration-domain-name. The value of a private-domain-name is a Printable String chosen from a set of such strings that is administered for this purpose by the country or ADMD alluded to above. [ISO]

Private management domain (PRMD) In the context of message handling, a management domain that comprises messaging system(s) managed (operated) by an organisation other than a service provider.

Note. – This does not preclude a service provider from managing (operating) a PRMD. [ITU-T]

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

Quality of service (QoS) Information relating to data transfer characteristics (for example, requested throughput and priority) used by a router to perform relaying and routing operations across the subnetworks which make up a network. [4]

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

Recipient See actual recipient. [ITU-T]

Recursion In the context of message handling, the situation that a message gets back to the same distribution list of origin and potentially circulates infinitely. [ITU-T]

Redirection In the context of message handling, a transmittal event in which an MTA replaces a user among a message's immediate recipients with a user preselected for that message. [ITU-T]

Registered access In the context of message handling services, access to the service performed by subscribers who have been registered by the service provider to use the service, and been allocated an O/R address. [ITU-T]

Report In the context of message handling, an instance of a secondary class of information object conveyed by means of message transfer. It is generated by the MTS; it reports the outcome or progress of a message's or probe's transmittal to one or more potential recipients. [ITU-T]

Retrieval In the context of message handling, a transmittal step in which a user's message store conveys a message or report to the user's UA. The user is an actual recipient of the message or the originator of the subject message or probe. [ITU-T]

Router The communication element that manages the relaying and routing of data while in transit from an originating end system to a destination end system. An ATN router comprises an OSI intermediate system and end system supporting a systems management agent. [4]

Routing A function within a layer that uses the address to which an entity is attached in order to define a path by which that entity can be reached. [4]

Routing domain A set of end systems and intermediate systems that operate the same routing protocols and procedures and that are wholly contained within a single administrative domain. A routing domain may be divided into multiple routing subdomains. [4]

Routing policy A set of rules that control the selection of routes and the distribution of routing information by ATN boundary intermediate systems (BISs). These rules are based on policy criteria rather than on performance metrics such as hop count, capacity, transit delay, cost, etc. which are usually applied for routing. There are two groups of routing policy in the ATN:

(1) general routing policy specified in the ATN Internet SARPs in order to ensure necessary connectivity in the ATN at a reasonable routing information update rate; and

(2) user-specified routing policy, i.e. individual policy rules which may be additionally implemented in ATN BISs by administrations and organisations to meet their specific operational and policy needs.

The set of rules in a BIS that determines the advertisement and use of routes is known as a routing policy. Each organisational user of the ATN must determine and apply their own routing policy. [4]

Safety case An analysis presenting an overall justification for the declaration that a particular systems satisfies its safety requirements. [4]

Security capabilities In the context of message handling, the mechanisms that protect against various security threats. [ITU-T]

Security management To support the application of security policies by means of functions which include the creation, deletion and control of security services and mechanisms, the distribution of security-relevant information and the reporting of security-related events. [4]

Specialised access In the context of message handling, the involvement of specialised access units providing intercommunication between message handling services and other telecommunication services. [ITU-T]

Standard attribute An attribute whose type is bound to a certain class of information. [ITU-T]

Subject In the context of message handling, the information, part of the header that summarises the content of the message as the originator has specified it. [ITU-T]

Subject message The message that is the subject of a report. [ITU-T]

Subject probe The probe that is the subject of a report. [ITU-T]

Submission Direct submission or indirect submission. [ITU-T]

Subnetwork An actual implementation of a data network that employs a homogeneous protocol and addressing plan, and is under control of a single authority. [4]

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

Systems management The set of functions related to the management of various OSI resources and their status across all layers of the OSI architecture. [4]

Transfer In the context of message handling, a transmittal step in which one MTA conveys a message, probe, or report to another. [ITU-T]

Transfer system A messaging system that contains one MTA; optionally one or more access units, and neither a UA nor a message store. [ITU-T]

Transmittal The conveyance or attempted conveyance of a message from its originator to its potential recipients, or of a probe from its originator to MTAs able to affirm any described message's deliverability to its potential recipients. It also encompasses the conveyance or attempted conveyance, to the originator of the message or probe, of any reports it provokes. It is a sequence of transmittal steps and events. [ITU-T]

User In the context of message handling, a functional object (e.g. a person), a component of the message handling environment, that engages in (rather than provides) message handling and that is a potential source or destination for the information objects an MHS conveys. [ITU-T]

User agent (UA) In the context of message handling, the functional object, a component of MHS, by means of which a single direct user engages in message handling. [ITU-T]

User requirements A description of what users expect to obtain from the system (not how the system should do it). They are usually expressed on a high level and do not include technical details. The direct user of the ATN is an application within an end system supporting air traffic management or aeronautical industry functions. The air traffic controller, other ground staff or the pilot are the human beings using directly, or indirectly, the ATN. The user may also be seen more on the abstract level as an organisation, e.g. airline or air navigation service provider. [4]

Validation In the ICAO context, a process that ensures that systems meet user requirements to an agreed level of confidence and can be produced from written SARPs and guidance material. One has to distinguish between performance based and functional validation. Single subsystems of the ATN, like routers, may be validated on a functional basis; validation of the ATN's suitability with respect to network performance etc. requires definition of performance requirements. [4]

XF-address An XF-address (translated address) is a particular MF-address of which the user within an AMHS Management Domain may be converted by an algorithmic method to and from an AF-address. [SARPs]

3. Definitions of elements of service

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

MT *Message Transfer*

IPM *Interpersonal Messaging*

PD *Physical Delivery*

MS *Message Store*

PR *Per recipient (available on a per-recipient basis)*

Access management 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.

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

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

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

1) all the attributes match precisely those of a subscriber UA. Delivery is attempted to that UA;

2) either insufficient attributes are supplied or those supplied match those of more than one subscriber UA. The message cannot be delivered;

3) at least the minimum set of attributes required by the destination MD is supplied. Nevertheless, taking all of the other attributes into account, the attributes match those of no UA.

In case 3) an MD that supports the alternate recipient assignment element of service can deliver the message to a UA that has been assigned to receive such messages. This UA will be notified of the 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.

Alternate recipient assignment 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 organisation can establish a UA to receive all messages for which country name, administration management domain name and organisation 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 organisation. This permits the organisation 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.

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

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

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

Auto-assignment of annotations This element of service enables an MS-user to instruct the MS to attach annotations to a selected message automatically, when the message is stored in the MS and satisfies specified criteria.

The MS-user may specify, through registration, several sets of selection criteria each of which may indicate the attachment of a different value of annotation. Subscription to this element of service requires subscription to the Stored Message Annotation element of service.

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

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

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

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

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

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

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

Auto-deletion after storage period This element of service enables an MS-user to instruct the MS to delete automatically any stored message whose storage period has elapsed. This registration remains in force until disabled by a subsequent registration. Messages that have not been listed or processed are not subject to auto-deletion.

Equally, entries of the Submission Log, Delivery Log, and Auto-action-log are not subject to auto-deletion. Other content-specific message handling Specifications may lay down additional rules for the performance of this element of service. Subscription to this element of service requires subscription to the Storage Period Assignment element of service.

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

Auto-forwarded indication 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.

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

Auto-forwarding of IP-messages This element of service enables an MS-user to instruct the MS to auto-forward selected IP-messages that are delivered to it. The MS-user may specify through registration several sets of criteria chosen from the attributes available in the MS, and IP-messages meeting each set of criteria will be auto-forwarded to one or more users or DLs. If requested by the message originator, a non-receipt notification is generated indicating that the IP-message was auto-forwarded, even if the MS retains a copy of the forwarded message. For each set of selection criteria, a body part may be specified, to be included as a “cover-note” with each auto-forwarded IP-message.

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

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

- not auto-submitted;
- auto-generated;
- auto-replied;
- auto-forwarded.

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

Blind copy recipient indication 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.

Body part encryption indication This element of service allows the originator to indicate to the recipient that a particular body part of the IP-message being sent has been encrypted. Encryption can be used to prevent unauthorised 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.61 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.86 stored message listing 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.

Content confidentiality 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.

Content integrity 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.

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

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

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

Should this and the conversion prohibition element of service both be selected, the latter shall take precedence.

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

Converted indication 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.

Copy precedence This element of service enables an originating UA to convey the precedence level (i.e. supplemental importance information) of a message as it applies to the copy recipients. Six levels of precedence are defined for this field (please see Table B.1 defined in B.131 below for specific values and their semantics).

The value of the copy precedence field must always be equal to, or of a lesser priority than the value of the primary precedence field.

Additional levels of precedence may be defined for national use. Upon receipt, the handling of unknown precedence levels will be dictated by the local "precedence handling policy".

Counter collection 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.

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

Cross-referencing indication 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.

Deferred delivery 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.

Deferred delivery cancellation 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.

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

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

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

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

Delivery time stamp indication 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.

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

Designation of recipient by directory name This element of service enables an originating UA to use a directory name in place of an individual recipient's O/R address.

Disclosure of other recipients This element of service enables the originating UA to instruct the MTS when 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.

Distribution code This element of service enables the originating UA to give distribution information to a recipient UA. The recipient UA can use this information to perform local distribution of a message to one or more persons or staff cells. This service contains two components, the Subject Indicator Code (SIC) and a distribution code, each of which is optional.

The SICs are bilaterally agreed codes that define the subject matter of a message to support onward distribution after delivery to a recipient organisation. Each SIC can consist of between three and eight characters. It is possible to attach up to eight SICs to a message.

The distribution code service the same function, but allows future use of object identifiers as the local distribution criteria. Any number of distribution codes may be specified. The assignment of the distribution code can be privately defined or may be subject to future standardisation.

Exempted address This element of service is used to convey the names of members of a DL that the originator has specified are to be excluded from receiving the message. Exclusion is performed at the point of DL expansion.

The names or addresses of exempted list members are also conveyed to the remaining recipient UAs. There is no guarantee that the exempted addresses will not receive the message as the result of redirection.

Extended authorisation information This element of service enables the originating UA to indicate to a recipient UA the date and time of some important event associated with the message, such as when the release of the message was formally approved. Depending upon local requirements, this date and time stamp may vary from the date and time when the message was submitted to the MTS. This element of service may be used in conjunction with B.5 to provide supplementary information.

Express mail service (EMS) 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.

Expiry date indication 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.

Explicit conversion 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.

Forwarded IP-message indication 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 multipart 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.

Grade of delivery selection 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.

Hold for delivery 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.

Implicit conversion 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.

Importance indication 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 categorisation 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.

Incomplete copy indication 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.

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

IP-message identification This element of service enables co-operating 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).

IPM-UA 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.

IPM-UA 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.

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

Latest delivery designation 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.

Message flow confidentiality 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.

Message identification 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.

Message instructions This element of service enables the originating UA to indicate to the recipient UA that message instructions (e.g. remarks) accompany the message. Examples of message instructions include special recipient handling requests, special body descriptions and bilateral information.

Message origin authentication 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.

Message security labelling 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.

Message sequence integrity 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.

Message type This service element enables receiving UAs to distinguish messages that relate to a specific project, contract, company position, press release, operation, exercise or drill. The service can convey a discrete identifier for each particular type plus optional printable information capable of identifying a particular project, press release, contract, company position, exercise, operation or drill. The value is provided by the originator.

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

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

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

Note. – The capability to store separate sets of registration information and to retrieve registered information was not defined in versions of this Recommendation published prior to 1996.

Multi-destination delivery 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.

Multi-part body 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.

Non-delivery notification 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) or in the case of access units, may indicate that the message was not received by the destination terminal. The reason the message was not delivered 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 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.

Note. – Non-delivery notifications are generated automatically, and do not depend on a request by an originator.

Non-receipt notification request indication 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-receipt notification, if either receipt notification or non-receipt notification was requested, 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.

Non-repudiation of content received This Element of Service enables a recipient of an IP-message to provide an irrevocable proof that the original IP-message content was received by the recipient.

This service provides irrevocable proof of the integrity of the content received and irrevocable proof of the authenticity of the recipient of the IP-message. This service fulfils the same function as the Proof of Content Received Element of Service, but in a manner which cannot be repudiated.

The corresponding irrevocable proof can be supplied in various ways depending on the security policy in force. The originator of the IP-notification always uses the "Non-repudiation of Origin" Element of Service when sending the IP-notification in response to the IP-message:

one way of providing the irrevocable proof is to incorporate the following in the IP-notification:

- A verified copy of the IP-message originator's "Non-repudiation of Origin" arguments (when present in the IP-message and verified by the recipient of the IP-message).
- A verified copy of the complete IP-message content, if the IP-message originator's "Non-repudiation of Origin" arguments are not present in the IP-message.

Note. – As an alternative to invoking this Element of Service, equivalent security may be achieved by the use of a notarisation mechanism, which requires bilateral agreement outside the scope of this Recommendation.
The recipient is required to fulfil the request for this Element of Service only when the UA is subject to a security policy which mandates the support of this element of service.

Non-repudiation of delivery 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.

Non-repudiation of IP-notification This Element of Service provides the recipient of a IP-notification with irrevocable proof of the identity of the originator of the IP-notification and with proof that the corresponding IP-message was received by the recipient.

This protects against any attempt by the recipient to deny subsequently that the IP-message was received or that the IP-notification was returned to the originator of the IP-message. This Element of Service fulfils the same service as Proof of IP-notification but in a manner which cannot be repudiated.

This Element of Service is used only in conjunction with Non-repudiation of Origin Element of Service applied to the IP-notification.

The corresponding irrevocable proof can be supplied in various ways depending on the security policy in force. One way of providing the irrevocable proof is by means of the MTS-user to MTS-user Data Origin Authentication Security Services defined in 10.2.1.1.1/X.402 and in ISO/IEC 10021-2 applied to the IP-notification, when the security service has non-repudiation properties.

The recipient is required to fulfil the request for this Element of Service only when the UA is subject to a security policy which mandates the support of this element of service.

Non-repudiation of origin 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.

Non-repudiation of submission 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.

Obsoleting indication 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.

Ordinary mail 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.

Original encoded information types indication 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.

Originator indication 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.

originator requested alternate recipient 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.

Originator reference This element of service enables the originating UA to indicate to a recipient UA a reference called the "originator's number". The originator's number may be used by the originating organisational unit as an internal reference. This service element is different from the identifier in that this reference is assigned by the originator, while the identifier is supplied by the UA.

Other recipients indicator The intent of this service element is to enable a recipient to determine which recipients are intended to receive the message without the use of MHS, as well as the category in which they are placed. While the primary and copy recipients indication service provides the names of recipients that can be reached through MHS, other recipients can be determined with this service element.

Note. – This service element does not allow the originator to convey the reason why the other recipient(s) will not receive the message via the MHS.

Physical delivery notification by MHS 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 authorised 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, 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.

Physical delivery notification by PDS 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 authorised 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, 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.

Physical forwarding allowed 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.

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

Primary and copy recipients indication 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.

Primary precedence This element of service enables an originating UA to convey the precedence level (i.e. supplemental importance) information of a message as it applies to the primary recipients. Six levels of precedence are defined for this element of service (see below for specific values and their semantics).

Additional levels of precedence may be defined for national use. Upon receipt, the handling of unknown precedence levels will be dictated by the local "precedence handling policy".

This service is provided not only as information from originator to recipient, but also is used to automatically select the MTS grade of delivery. The six levels of precedence are mapped to only three levels of grade of delivery which is conveyed in the MTS envelope. Table B.1 maps primary precedence values onto the MTS priority protocol element. Behaviour upon receipt is determined by local policy.

TABLE B.1/F.400

Primary precedence value mapping onto the MTS Priority EOS

Primary Precedence	MTS EOS Priority
Override (5)	Urgent (2)
Flash (4)	Urgent (2)
Immediate (3)	Normal (0)
Priority (2)	Normal (0)
Routine (1)	Non-urgent (1)
Deferred (0)	Non-urgent (1)

Note. – Elements of service specific to EDI messaging and voice messaging are defined in Recommendations F.435 and F.440.

Probe 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.

Probe origin authentication 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.

Proof of content received This Element of Service enables a recipient of an IP-message to provide proof that the original IP-message content was received by the recipient. This service provides proof of the integrity of the content received and proof of the authenticity of the recipient of the IP-message.

This Element of Service is used only in conjunction with "Content Integrity" and/or "Message Origin Authentication" Elements of Service applied to the subject IP-notification.

The corresponding proof can be supplied in various ways depending on the security policy in force. The originator of the IP-notification always uses the "Content Integrity" and/or "Message Origin Authentication" Element of Service when sending the receipt IP-notification in response to the IP-message.

One way of providing the proof is to incorporate the following in the IP-notification:

- A verified copy of the IP-message originator's "Content Integrity" and/or "Message Origin Authentication" arguments (when present in the IP-message and verified by the recipient of the IP-message).
- A verified copy of the complete original IP-message content, if the IP-message originator's "Content Integrity" and/or "Message Origin Authentication" arguments are not present in the IP-message.

The recipient is required to fulfil the request for this Element of Service only when the UA is subject to a security policy which mandates the support of this element of service.

Note 1: The "Message Origin Authentication" Element of Service may be provided on a per message basis using the Message-origin-authentication-check and/or on a per recipient basis using the Message-token as defined in Recommendation X.411 | ISO/IEC 10021-4.

Note 2: The "Content Integrity" Element of Service may be conveyed in several places on the message envelope. The Content-integrity-check can be stand-alone security argument in the message envelope and/or attributes of the Message-token as defined in Recommendation X.411 and ISO/IEC 10021-4.

Proof of delivery 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.

Proof of IP-notification This Element of Service provides the originator of an IP-message with proof that the IP-message was received by its recipient, and that the recipient was the originator of the received IP-notification.

This protects against any attempt by the recipient IPM-UA to deny subsequently that the IP-message was received and that the IP-notification was returned to the originator.

This Element of Service is used only in conjunction with "Content Integrity" and /or the "Message Origin Authentication" Element of Service applied to the IP-notification.

The corresponding proof can be supplied in various ways depending on the security policy in force. One way of providing the proof is by means of the MTS-user to MTS-user Data Origin Authentication Security Services, defined in 10.2.1.1.1/X.402 and in ISO/IEC 10021-2, applied to the IP-notification.

The recipient is required to fulfil the request for this Element of Service only when the UA is subject to a security policy which mandates the support of this element of service.

Proof of submission 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.

Receipt notification request indication This element of service allows the originator to ask that he be notified when the IP-message being sent is received by the recipient's UA. 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.

Redirection disallowed by originator 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.

Redirection of incoming message This element of service enables a UA, through registration, 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 require delivery to the intended recipient before redirection can take place. It is therefore distinct from the Auto-forwarding of IP-messages element of service.

Note 2: Different incoming messages, on the basis of their content-types, security labels, and other criteria, may be redirected to separate alternate recipients or not redirected at all.

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

Registered mail to addressee in person 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.

Reply request indication 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.

Replying IP-message indication 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.

Report origin authentication 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.

Request for forwarding address 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.

Requested preferred delivery method 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).

Note. – This assumes availability of a directory and specification of a directory name by the originator together with this element of service. It may not be possible to match the request with the O/R address available in the directory. Non-delivery may occur if no feasible match can be found.

Request for non-repudiation of content received This Element of Service enables the originator of an IP-message to request the recipient of the IP-message to provide an irrevocable proof of the received IP-message content by means of an IP-notification.

This Element of Service may be subscribed to only if the Receipt Notification Request Indication Element of Service is subscribed to.

If this Element of Service is requested, the Request for Proof of Content Received Element of Service shall not be requested.

This Element of Service provides only an indication of the originator's request. Fulfilment of the request requires support of the Non-repudiation of Content Received Element of Service.

Request for non-repudiation of IP-notification This Element of Service enables the originator of an IP-message to request the recipient of the IP-message to provide irrevocable proof of the origin of an IP-notification generated in response to the IP-message.

This Element of Service may be subscribed to only if the Receipt Notification Request Indication Element of Service is subscribed to.

If this Element of Service is requested, the Request for Proof of IP-notification Element of Service shall not be requested.

This Element of Service provides only an indication of the originator's request. Fulfilment of the request requires support of the Non-repudiation of IP-notification Element of Service.

Request for proof of content received This Element of Service enables the originator of the IP-message to request the recipient of the IP-message to provide proof of the received IP-message content by means of an IP-notification.

This Element of Service may be subscribed to only if the Receipt Notification Request Indication Element of Service is subscribed to.

This Element of Service provides only an indication of the originator's request. Fulfilment of the request requires support of the Proof of Content Received Element of Service.

Request for proof of IP-notification This Element of Service enables the originator of the IP-message to request the recipient of the IP-message to provide proof of the origin of an IP-notification generated in response to the IP-message.

This Element of Service may be subscribed to only if the Receipt Notification Request Indication Element of Service is subscribed to.

This Element of Service provides only an indication of the originator's request. Fulfilment of the request requires support of the Proof of IP-notification Element of Service.

Restricted delivery This element of service enables a recipient UA to indicate to the MTS, through registration, that it is not prepared to accept delivery of messages which originate from, or are redirected by, or are DL-expanded by certain MTS-users.

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

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

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

Note 2: The MTS abstract service specified in Recommendation X.411 and ISO/IEC 10021-4 does not provide a technical realisation of this element of service. Its provision is for further study.

Return of content 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.

Sensitivity indication 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's originator.
- Company-confidential: The IP-message contains information that should be treated according to company-specific procedures.

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

Stored message alert 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 satisfies 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.

Stored message annotation This element of service enables an MS-user to attach one or more textual annotations to a stored message. Annotations apply to the complete message and may not be applied selectively to different parts of the message. Annotations are local to the MS and MS-user and are not transmitted through the MTS in any message. The “cover note” described in B.83 is not related to message annotations.

Stored message deletion This element of service enables a recipient UA to delete certain of its messages from the MS. Subject to subscription, deletion may be restricted to messages meeting certain criteria, e.g. messages stored for longer than an agreed period of time. Messages cannot be deleted if they have not been previously listed.

Stored message fetching 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.

Stored message grouping This element of service enables an MS-user to attach group-names to messages stored in the MS. A message can have zero, one, or more group-names associated with it that can subsequently be used for selection purposes. Each message group-name comprises a sequence of components which may be regarded as modelling a storage hierarchy. The setting, changing, or deletion of the group-names attached to a message can be performed by the MS-user.

The UA indicates to the MS, through registration, the name of each distinct group which the UA will employ to label each group of related messages. Each group-name may be assigned a descriptive text registered together with the group-name. The MS will verify that the group-names subsequently employed by the user belong to the registered set of group-names, and will prevent the user from deregistering group-names which are currently attached to stored messages, or which are registered for use by the Auto-assignment of Group Names element of service. A group-name remains valid until it is deregistered. The MS will prohibit an attempt to register the same group-name twice.

Stored message summary 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.

Storage of draft messages This element of service enables an MS-user to store draft messages in the MS. The user may obtain summaries of draft messages and may access a draft message by means of the Stored Message Listing and Stored Message Fetching elements of service.

Storage on submission This element of service enables an MS-user to instruct the MS to store a copy of a message upon its submission, either by the MS-user or as a result of the performance of an auto-action. Storage of a submitted message is conditional upon the success of the submission. The user may instruct the MS to store all submitted messages, or may control storage on a per message basis.

Storage period assignment This element of service enables an MS-user to assign a storage period to a stored message. The storage period indicates the period of time for which the user anticipates the message should be retained in the MS; this may be expressed as a period of time (from the start of storage), or as an absolute date and time. This element of service must be subscribed to if the Auto-deletion after Storage Period or Auto-assignment of Storage Period elements of service are subscribed to.

Subject indication 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.

Submission log This element of service enables an MS-user to access a log that records details of the messages submitted from the MS to the MTS. These records are generated regardless of whether a copy of the submitted message is stored by means of the Storage on Submission element of service. Even where a copy is stored, the corresponding Submission Log entry may persist after the message has been deleted. Both successful and unsuccessful submissions are recorded. A Submission Log entry contains a subset of the information that may be stored for a submitted message.

The quantity of information stored in the Submission Log for each message is specified at subscription time. The MS-user is able to determine whether the submitted message corresponding to a Submission Log entry has been deleted. The MS-user is able to retrieve information from the Submission Log by means of the Stored Message Listing, Stored Message Fetching and Stored Message Summary elements of service. The ability to delete Submission Log entries is subject to subscription, and may be restricted to messages meeting certain criteria, e.g. messages stored longer than an agreed period of time.

Submission of IP-messages incorporating stored messages This element of service enables an MS-user to instruct the MS to incorporate parts of one or more stored messages as body parts of a submitted IP-message. The submitted IP-message may also contain body parts supplied in the submission from the MS-user.

The stored message which is the source of a body part may be a delivered, submitted or draft message. Individual body parts or the whole content of a stored IP-message may be incorporated. When the content is incorporated it will form a Forwarded IP-message. Delivery-information may also be incorporated from delivered messages when the content is incorporated.

The MS may optionally support the forwarding of body parts from messages which are not IP-messages. In this case, only body parts whose definition is compatible with IPM (or for which rules of conversion into IPM body parts are defined) may be forwarded. The complete content of a message cannot be forwarded if the message is not an IP-message.

The message submitted to the MTS, incorporating the stored messages or body parts may be stored in the MS if the user subscribes to the Storage on Submission element of service. An extract of the message will also be stored in the Submission Log if this element of service is subscribed to.

Submission time stamp indication 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.

Typed body 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.

Note 1: One example is the use of a file transfer body part. This provides for conveying the contents of a stored file and other information associated with the file from originator to recipient. The other information includes:

- *file attributes, which are typically stored along with the file contents;*
- *information on the environment from which the transfer originated;*
- *references to existing stored files or earlier messages.*

Note 2: Another example is the use of a voice body part.

Undeliverable mail with return of physical message 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.

Use of distribution list This element of service enables an originating UA to specify a distribution list in place of all the individual recipients (users or nested DLs) 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.

User/UA capabilities registration This element of service enables a UA to indicate to its MTA, through registration, the categories of message it is capable of handling, and which MTA may deliver to it. A message category is defined as a combination of various properties:

1) the content type(s) of messages which may be delivered;
2) the encoded information type(s) of messages which may or may not be delivered;
3) additional properties, including the maximum message length, and the security labels present.

Note. – It is possible to register certain encoded information types such that they cause a message to be delivered regardless of the other encoded information types present. A user may declare certain encoded information types undeliverable to cause the MTS to perform implicit conversion.

The UA may specify different sets of registration information to control the delivery of different categories of message.
The MTA will not deliver to a UA a message that does not match, or exceeds, the capabilities registered.

END of Appendix A