INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

F.400/X.400

Amendment 1
(09/98)

SERIES F: NON-TELEPHONE TELECOMMUNICATION SERVICES

Message handling services

SERIES X: DATA NETWORKS AND OPEN SYSTEM COMMUNICATIONS

Message Handling Systems

Message handling system and service overview

Amendment 1

ITU-T Recommendation F.400/X.400 – Amendment 1

(Previously CCITT Recommendation)

ITU-T F-SERIES RECOMMENDATIONS

NON-TELEPHONE TELECOMMUNICATION SERVICES

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

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

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS AND OPEN SYSTEM COMMUNICATIONS

PUBLIC DATA NETWORKS	
Services and facilities	X.1–X.19
Interfaces	X.20–X.49
Transmission, signalling and switching	X.50–X.89
Network aspects	X.90–X.149
Maintenance	X.150–X.179
Administrative arrangements	X.180–X.199
OPEN SYSTEMS INTERCONNECTION	
Model and notation	X.200–X.209
Service definitions	X.210–X.219
Connection-mode protocol specifications	X.220–X.229
Connectionless-mode protocol specifications	X.230–X.239
PICS proformas	X.240–X.259
Protocol Identification	X.260–X.269
Security Protocols	X.270–X.279
Layer Managed Objects	X.280–X.289
Conformance testing	X.290–X.299
INTERWORKING BETWEEN NETWORKS	
General	X.300–X.349
Satellite data transmission systems	X.350–X.399
MESSAGE HANDLING SYSTEMS	**X.400–X.499**
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	
Networking	X.600–X.629
Efficiency	X.630–X.639
Quality of service	X.640–X.649
Naming, Addressing and Registration	X.650–X.679
Abstract Syntax Notation One (ASN.1)	X.680–X.699
OSI MANAGEMENT	
Systems Management framework and architecture	X.700–X.709
Management Communication Service and Protocol	X.710–X.719
Structure of Management Information	X.720–X.729
Management functions and ODMA functions	X.730–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	
Commitment, Concurrency and Recovery	X.850–X.859
Transaction processing	X.860–X.879
Remote operations	X.880–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999

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

ITU-T RECOMMENDATION F.400/X.400

MESSAGE HANDLING SYSTEM AND SERVICE OVERVIEW

AMENDMENT 1

Summary

This amendment contains enhancements on the organizational mapping, on various tables regarding elements of service and, in Annex B, an alphabetical re-ordering of the definitions of elements of service.

Source

Amendment 1 to ITU-T Recommendation F.400/X.400 was prepared by ITU-T Study Group 7 (1997-2000) and was approved under the WTSC Resolution No. 1 procedure on the 25th of September 1998.

FOREWORD

ITU (International Telecommunication Union) is the United Nations Specialized Agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of the ITU. The ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Conference (WTSC), which meets every four years, establishes the topics for study by the ITU-T Study Groups which, in their turn, produce Recommendations on these topics.

The approval of Recommendations by the Members of the ITU-T is covered by the procedure laid down in WTSC Resolution No. 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation the term *recognized operating agency (ROA)* includes any individual, company, corporation or governmental organization that operates a public correspondence service. The terms *Administration*, *ROA* and *public correspondence* are defined in the *Constitution of the ITU (Geneva, 1992)*.

INTELLECTUAL PROPERTY RIGHTS

The ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. The ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, the ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

CONTENTS

Recommendation F.400/X.400

MESSAGE HANDLING SYSTEM AND SERVICE OVERVIEW

AMENDMENT 1

(Geneva, 1998)

1) Clause 4, Abbreviations

Replace the abbreviation "RPOA" by "ROA" as follows:

ROA Recognized Operating Agency

2) Figure 5/F.400 – "Relationship between management domains"

Replace the dotted lines by bold lines and substitute the "Notes" as follows:

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

NOTE 2 – PRMD 1 has connections to two ADMDs within country A.

PRMD 2 spans a country border, and has connections to an ADMD in each country.

PRMD 3 has multiple connections to ADMD 3.

PRMD 4 is only connected to other MDs by relaying through PRMD 1.

PRMD 5 has connections to other PRMDs, both within the same country (to PRMD 3) and internationally (to PRMD 1).

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

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

3) Subclause 8.5, "Message Store"

Replace the current text by the following:

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

4) Subclause 11.1, "Introduction"

Append the following Note to the end of the current text:

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

5) Subclause 12.2, "directory names:"

Replace the lower case "d" by an upper case one, remove ":" and enter two lines at the end of the title.

6) Subclause 12.3, "O/R names:"

Remove ":" and enter two lines at the end of the title.

7) Subclause 12.4, "O/R addresses:"

Remove ":" and enter two lines at the end of the title.

8) Table 2/F.400 – "Provision and use of secure messaging elements of service by MHS components"

Remove the last sentence "R The MHS component is a requester of the service".

9) Subclause 15.7, IPM Security,

Append the following table to the end of the text:

Table 3/F.400/X.400 – Provision and use of additional secure messaging elements of service by IPM-UAs

Elements of service	IP-message originator	MTS	IP-message recipient
Request for Non-repudiation of Content Received	Requester	–	User
Non-repudiation of Content Received	User	–	Provider
Request for Non-repudiation of IP-notification	Requester	–	User
Non-repudiation of IP-notification	User	–	Provider
Request for Proof of Content Received	Requester	–	User
Proof of Content Received	User	–	Provider
Request for Proof of IP-notification	Requester	–	User
Proof of IP-notification	User	–	Provider

10) Clause 16, "Conversion in MHS"

Append the following to the current text:

The conversion process for IP-messages can be performed on body parts of specific types if they are present in a message. The general aspects of conversion and the specific conversion rules for conversion between different EITs are detailed in Recommendation X.408. Recommendation X.408 deals with conversion including the following: IA5 Text, G3Fax, G4 Class1, and Videotex.

11) Clause 18, "Elements of Service – Purpose"

Replace the word "Table 3" by "Table 4" in the beginning of the fourth paragraph, and replace "Table 3/F.400 MHS elements of service" by "Table 4/F.400/X.400 – MHS elements of service" as follows:

Table 4/F.400/X.400 – MHS elements of service

Elements of service	MT	IPM	PD	MS	Annex B reference
Access management	X				B.1
Additional physical rendition			X		B.2
Alternate recipient allowed	X				B.3
Alternate recipient assignment	X				B.4
Authorization time indication		X			B.5
Authorizing users indication		X			B.6

Table 4/F.400/X.400 – MHS elements of service *(continued)*

Elements of service	MT	IPM	PD	MS	Annex B reference
Auto-acknowledgment of IP-messages		X		X	B.7
Auto-action Log				X	B.8
Auto-advise		X		X	B.9
Auto-assignment of Annotations				X	B.10
Auto-assignment of Group Names				X	B.11
Auto-assignment of Storage Period				X	B.12
Auto-correlation of IP-messages		X		X	B.13
Auto-correlation of IP-notifications		X		X	B.14
Auto-correlation of Reports				X	B.15
Auto-deletion after Storage Period				X	B.16
Auto-discarding of IP-messages		X		X	B.17
Auto-forwarded indication		X			B.18
Auto-forwarding of IP-messages		X		X	B.19
Auto-submitted indication		X			B.20
Basic physical rendition			X		B.21
Blind copy recipient indication		X			B.22
Body part authentication and integrity		X			B.23
Body part encryption		X			B.24
Circulation list recipients indication		X			B.25
Content confidentiality	X				B.26
Content integrity	X				B.27
Content type indication	X				B.28
Conversion prohibition	X				B.29
Conversion prohibition in case of loss of information	X				B.30
Converted indication	X				B.31
Counter collection			X		B.32
Counter collection with advice			X		B.33
Cover page suppression	X				B.34
Cross-referencing indication		X			B.35
Deferred delivery	X				B.36
Deferred delivery cancellation	X				B.37
Delivery log				X	B.38
Delivery notification	X				B.39
Delivery time stamp indication	X				B.40
Delivery via bureaufax service			X		B.41
Designation of recipient by directory name	X				B.42
Disclosure of other recipients	X				B.43
Distribution codes indication		X			B.44
DL-exempted recipients	X				B.45
DL-expansion history indication	X				B.46
DL-expansion prohibited	X				B.47

Table 4/F.400/X.400 – MHS elements of service *(continued)*

Elements of service	MT	IPM	PD	MS	Annex B reference
EMS (Express Mail Service)			X		B.48
Expiry date indication		X			B.49
Explicit conversion	X				B.50
Forwarded IP-message indication		X			B.51
Grade of delivery selection	X				B.52
Hold for delivery	X				B.53
Implicit conversion	X				B.54
Importance indication		X			B.55
Incomplete copy indication		X			B.56
Information category indication		X			B.57
IP-message Action Status		X		X	B.58
IP-message identification		X			B.59
IP-message security labelling		X			B.60
Language indication		X			B.61
Latest delivery designation	X				B.62
Manual handling instructions indication		X			B.63
Message flow confidentiality	X				B.64
Message identification	X				B.65
Message origin authentication	X				B.66
Message security labelling	X				B.67
Message sequence integrity	X				B.68
MS register				X	B.69
Multi-destination delivery	X				B.70
Multi-part body		X			B.71
Non-delivery notification	X				B.72
Non-receipt notification request indication		X			B.73
Non-repudiation of content received		X			B.74
Non-repudiation of delivery	X				B.75
Non-repudiation of IP-notification		X			B.76
Non-repudiation of origin	X				B.77
Non-repudiation of submission	X				B.78
Obsoleting indication		X			B.79
Ordinary mail			X		B.80
Original encoded information types indication	X				B.81
Originator indication		X			B.82
Originator reference indication		X			B.83
Originator requested alternate recipient	X				B.84
Physical delivery notification by MHS			X		B.85
Physical delivery notification by PDS			X		B.86
Physical forwarding allowed			X		B.87
Physical forwarding prohibited			X		B.88
Precedence indication		X			B.89
Prevention of non-delivery notification	X				B.90

Table 4/F.400/X.400 – MHS elements of service *(concluded)*

Elements of service	MT	IPM	PD	MS	Annex B reference
Primary and copy recipients indication		X			B.91
Probe		X			B.92
Probe origin authentication	X				B.93
Proof of content received		X			B.94
Proof of delivery	X				B.95
Proof of IP-notification		X			B.96
Proof of submission	X				B.97
Receipt notification request indication		X			B.98
Redirection disallowed by originator	X				B.99
Redirection of incoming messages	X				B.100
Registered mail			X		B.101
Registered mail to addressee in person			X		B.102
Reply request indication		X			B.103
Replying IP-message indication		X			B.104
Report origin authentication	X				B.105
Request for forwarding address			X		B.106
Request for non-repudiation of content received		X			B.107
Request for non-repudiation of IP-notification		X			B.108
Request for proof of content Received		X			B.109
Request for proof of IP-notification		X			B.110
Requested preferred delivery method	X				B.111
Restricted delivery	X				B.112
Return of content	X				B.113
Secure access management	X				B.114
Sensitivity indication		X			B.115
Special delivery			X		B.116
Storage of draft messages				X	B.117
Storage on submission				X	B.118
Storage period assignment				X	B.119
Stored message alert				X	B.120
Stored message annotation				X	B.121
Stored message deletion				X	B.122
Stored message fetching				X	B.123
Stored message grouping				X	B.124
Stored message listing				X	B.125
Stored message summary				X	B.126
Subject indication		X			B.127
Submission log				X	B.128
Submission of IP-messages incorporating stored messages		X		X	B.129
Submission time stamp indication	X				B.130
Typed body		X			B.131
Undeliverable mail with return of physical message			X		B.132
Use of distribution list	X				B.133
User/UA capabilities registration	X				B.134

12) Subclause 19.2, "Basic Message Transfer service"

Replace the word "Table 4" by "Table 5" in the sentence before the last sentence of the paragraph, and replace "Table 4/F.400" by "Table 5/F.400/X.400" as follows:

Table 5/F.400/X.400 – Elements of service belonging to the basic MT service

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

13) Subclause 19.3, "MT service optional user facilities"

Replace the words "Table 5" and "Tables 6 to 9" by "Table 6" and "Tables 7 to 10" respectively, and replace "Table 5/F.400" by "Table 6/F.400/X.400" as follows:

Table 6/F/400/X.400 – MT service optional user facilities

Elements of service	Classification	Available	Annex B reference
Alternate recipient allowed	E	PM	B.3
Alternate recipient assignment	A	CA	B.4
Content confidentiality	A	PM	B.26
Content integrity	A	PM	B.27
Conversion prohibition	E	PM	B.29
Conversion prohibition in case of loss of information	A	PM	B.30
Cover page suppression	A	PM	B.34
Deferred delivery	E	PM	B.36
Deferred delivery cancellation	E	PM	B.37
Delivery notification	E	PM	B.39
Designation of recipient by directory name	A	PM	B.42
Disclosure of other recipients	E	PM	B.43
DL-exempted recipients	A	PM	B.45
DL-expansion history indication	A	PM	B.46
DL-expansion prohibited	A	PM	B.47
Explicit conversion	A	PM	B.50
Grade of delivery selection	E	PM	B.52
Hold for delivery	A	CA	B.53
Implicit conversion	A	CA	B.54
Latest delivery designation	A	PM	B.62
Message flow confidentiality	A	PM	B.64

Table 6/F/400/X.400 – MT service optional user facilities *(concluded)*

Elements of service	Classification	Available	Annex B reference
Message origin authentication	A	PM	B.66
Message security labelling	A	PM	B.67
Message sequence integrity	A	PM	B.68
Multi-destination delivery	E	PM	B.70
Non-repudiation of delivery	A	PM	B.75
Non-repudiation of origin	A	PM	B.77
Non-repudiation of submission	A	PM	B.78
Originator requested alternate recipient	A	PM	B.84
Prevention of non-delivery notification	A	PM	B.90
Probe	A	PM	B.92
Probe origin authentication	A	PM	B.93
Proof of delivery	A	PM	B.95
Proof of submission	A	PM	B.97
Redirection disallowed by originator	A	PM	B.99
Redirection of incoming messages	A	PM	B.100
Report origin authentication	A	PM	B.105
Requested preferred delivery method	A (Note)	PM	B.111
Restricted delivery	A	PM	B.112
Return of content	A	PM	B.113
Secure access management	A	CA	B.114
Use of distribution list	A	PM	B.133
NOTE – Does not imply the provision of all delivery methods which may be requested.			

14) Subclause 19.4, "Base MH/PD service intercommunication"

Replace the words "Table 6" by "Table 7", and replace "Table 6/F.400" by "Table 7/F.400/X.400" as follows:

Table 7/F.400/X.400 – Elements of service belonging to the base MH/PD service intercommunication

Elements of service	Annex B reference
Basic physical rendition	B.21
Ordinary mail	B.80
Physical forwarding allowed	B.87
Undeliverable mail with return of physical message	B.132

15) Subclause 19.5, "Optional user facilities for MH/PD service intercommunication"

Replace the words "Table 7" by "Table 8", and replace "Table 7/F.400" by "Table 8/F.400/X.400" as follows:

Table 8/F.400/X.400 – Optional user facilities for MH/PD service intercommunication

Elements of service	Classification	Annex B reference
Additional physical rendition	A	B.2
Counter collection	E	B.32
Counter collection with advice	A	B.33
Delivery via bureaufax service	A	B.41
EMS (Express Mail Service)[a)]	E	B.48
Physical delivery notification by MHS	A	B.85
Physical delivery notification by PDS	A	B.86
Physical forwarding prohibited	A	B.88
Registered mail	A	B.101
Registered mail to addressee in person	A	B.102
Request for forwarding address	A	B.106
Special delivery [a)]	E	B.116
a) At least one or the other element of service shall be supported by the PDAU and the associated PDS.		

16) Subclause 19.6, "Base message store"

Replace the words "Table 8" by "Table 9", and replace "Table 8/F.400" by "Table 9/F.400/X.400" as follows:

Table 9/F.400/X.400 – Base message store

Elements of service	Annex B reference
MS register	B.69
Stored message deletion	B.122
Stored message fetching	B.123
Stored message listing	B.125
Stored message summary	B.126

17) Subclause 19.7, "MS optional user facilities"

Replace the words "Table 9" by "Table 10", and replace "Table 9/F.400" by "Table 10/F.400/X.400" as follows:

Table 10/F.400/X.400 – MS optional user facilities

Elements of service	Classification	Annex B reference
Auto-action Log	A	B.8
Auto-assignment of Annotations	A	B.10
Auto-assignment of Group Names	A	B.11
Auto-assignment of Storage Period	A	B.12
Auto-correlation of Reports	A	B.15
Auto-deletion after Storage Period	A	B.16
Delivery log	A	B.38
Storage of draft messages	A	B.117
Storage on submission	A	B.118
Storage period assignment	A	B.119
Stored message alert	A	B.120
Stored message annotation	A	B.121
Stored message grouping	A	B.124
Submission log	A	B.128

18) Subclause 19.8, "Basic interpersonal messaging service"

Replace the words "Table 10" by "Table 11", and replace "Table 10/F.400" by "Table 11/F.400/X.400" as follows:

Table 11/F.400/X.400 – Elements of service belonging to the basic IPM service

Elements of service	Annex B reference
Access management	B.1
Content type indication	B.28
Converted indication	B.31
Delivery time stamp indication	B.40
IP-message identification	B.59
Message identification	B.65
Non-delivery notification	B.72
Original encoded information types indication	B.81
Submission time stamp indication	B.130
Typed body	B.131
User/UA capabilities registration	B.134

19) Subclause 19.9, "IPM service optional user facilities"

Replace the words "Tables 11 and 12 " by "Tables 12 and 13" respectively in the first sentence of the text, and replace "Table 11/F.400" by "Table 12/F.400/X.400" and "Table 12/F.400" by "Table 13/F.400/X.400" as follows:

Table 12/F.400/X.400 – IPM optional user facilities selectable on a per-message basis

Elements of service	Origination	Reception	Annex B reference
Additional physical rendition	A	A	B.2
Alternate recipient allowed	A	A	B.3
Authorization time indicator	A	A	B.5
Authorizing users indication	A	E	B.6
Auto-forwarded indication	A	E	B.18
Auto-submitted indication	A	E	B.20
Basic physical rendition	A	E*	B.21
Blind copy recipient indication	A	E	B.22
Body part authentication and integrity	A	A	B.23
Body part encryption	A	E	B.24
Circulation list recipients indication	A	A	B.25
Content confidentiality	A	A	B.26
Content integrity	A	A	B.27
Conversion prohibition	E	E	B.29
Conversion prohibition in case of loss of information	A	A	B.30
Counter collection	A	E*	B.32
Counter collection with advice	A	A	B.33
Cover page suppression	A	A	B.34
Cross-referencing indication	A	E	B.35
Deferred delivery	E	N/A	B.36
Deferred delivery cancellation	A	N/A	B.37
Delivery notification	E	N/A	B.39
Delivery via bureaufax service	A	A	B.41
Designation of recipient by directory name	A	N/A	B.42
Disclosure of other recipients	A	E	B.43
Distribution codes indication	A	A	B.44
DL-exempted recipients	A	A	B.45
DL-expansion history indication	N/A	E	B.46
DL-expansion prohibited	A	N/A	B.47
EMS (Express Mail Service)	A	E*	B.48
Expiry date indication	A	E	B.49
Explicit conversion	A	N/A	B.50
Forwarded IP-message indication	A	E	B.51
Grade of delivery selection	E	E	B.52
Importance indication	A	E	B.55
Incomplete copy indication	A	A	B.56

Table 12/F.400/X.400 – IPM optional user facilities selectable on a per-message basis *(continued)*

Elements of service	Origination	Reception	Annex B reference
Information category indication	A	A	B.57
IP-message security labelling	A	A	B.60
Language indication	A	A	B.61
Latest delivery designation	A	N/A	B.62
Manual handling instructions indication	A	A	B.63
Message flow confidentiality	A	N/A	B.64
Message origin authentication	A	A	B.66
Message security labelling	A	A	B.67
Message sequence integrity	A	A	B.68
Multi-destination delivery	E	N/A	B.70
Multi-part body	A	E	B.71
Non-receipt notification request indication	A	E	B.73
Non-repudiation of content received	A	A	B.74
Non-repudiation of delivery	A	A	B.75
Non-repudiation of IP-notification	A	A	B.76
Non-repudiation of origin	A	A	B.77
Non-repudiation of submission	A	N/A	B.78
Obsoleting indication	A	E	B.79
Ordinary mail	A	E*	B.80
Originator indication	E	E	B.82
Originator reference indication	A	A	B.83
Originator requested alternate recipient	A	N/A	B.84
Physical delivery notification by MHS	A	A	B.85
Physical delivery notification by PDS	A	E*	B.86
Physical forwarding allowed	A	E*	B.87
Physical forwarding prohibited	A	E*	B.88
Precedence indication	A	A	B.89
Prevention of non-delivery notification	A	N/A	B.90
Primary and copy recipients indication	E	E	B.91
Probe	A	N/A	B.92
Probe origin authentication	A	N/A	B.93
Proof of content received	A	A	B.94
Proof of delivery	A	A	B.95
Proof of IP-notification	A	A	B.96
Proof of submission	A	N/A	B.97
Receipt notification request indication	A	A	B.98
Redirection disallowed by originator	A	N/A	B.99
Registered mail	A	A	B.101
Registered mail to addressee in person	A	A	B.102
Reply request indication	A	E	B.103
Replying IP-message indication	E	E	B.104

Table 12/F.400/X.400 – IPM optional user facilities selectable on a per-message basis *(concluded)*

Elements of service	Origination	Reception	Annex B reference
Report origin authentication	A	A	B.105
Request for forwarding address	A	A	B.106
Request for non-repudiation of content received	A	A	B.107
Request for non-repudiation of IP-notification	A	A	B.108
Request for proof of content received	A	A	B.109
Request for proof of IP-notification	A	A	B.110
Requested preferred delivery method	A	A	B.111
Return of content	A	N/A	B.113
Sensitivity indication	A	E	B.115
Special delivery (Note)	A	E*	B.116
Storage of draft messages	N/A	A	B.117
Storage on submission	N/A	A	B.118
Storage period assignment	N/A	A	B.119
Stored message annotation	N/A	A	B.121
Stored message deletion	N/A	E***	B.122
Stored message fetching	N/A	E***	B.123
Stored message grouping	N/A	A	B.124
Stored message listing	N/A	E**	B.125
Stored message summary	N/A	E**	B.126
Subject indication	E	E	B.127
Submission of IP-messages incorporating stored messages	N/A	A	B.129
Undeliverable mail with return of physical message	A	E*	B.132
Use of distribution list	A	N/A	B.133

E Essential optional user facility has to be provided

E* Essential optional user facility only applying to PDAUs

E** Essential optional user facility applying to MSs. Additional optional user facility applying to UAs (which connect to MSs)

E*** Essential optional user facility applying to MSs and UAs

A Additional optional user facility can be provided

N/A Not applicable

NOTE – At least EMS or Special Delivery shall be supported by the PDAU and associated PDS

Table 13/F.400/X.400 – IPM optional user facilities agreed for a contractual period of time

Elements of service	Classification	Annex B reference
Alternate recipient assignment	A	B.4
Auto-acknowledgment of IP-messages	A	B.7
Auto-action Log	A	B.8
Auto-advise	A	B.9
Auto-assignment of Annotations	A	B.10
Auto-assignment of Group Names	A	B.11
Auto-assignment of Storage Period	A	B.12
Auto-correlation of IP-messages	A	B.13
Auto-correlation of IP-notifications	A	B.14
Auto-correlation of Reports	A	B.15
Auto-deletion after Storage Period	A	B.16
Auto-discarding of IP-messages	A	B.17
Auto-forwarding of IP-messages	A	B.19
Delivery Log	A	B.38
Hold for delivery	A	B.53
Implicit conversion	A	B.54
IP-message Action Status	A	B.58
MS register	A	B.69
Redirection of incoming messages	A	B.100
Restricted delivery	A	B.112
Secure access management	A	B.114
Stored message alert	A	B.120
Submission Log	A	B.128

20) Annex B

Replace the whole content by the alphabetical re-ordered text of the "Definitions of Elements of Service" as follows:

Annex B

Definitions of elements of service

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

MT Message Transfer

IPM Interpersonal Messaging

PD Physical Delivery

MS Message Store

MS-94 1994 enhanced Message Store

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

B.1 access management MT

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

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

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

B.2 additional physical rendition PD PR

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

B.3 alternate recipient allowed MT

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

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

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

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

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

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

B.4 alternate recipient assignment MT

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

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

B.5 authorization time indication IPM

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

B.6 authorizing users indication IPM

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

B.7 auto-acknowledgement of IP-messages IPM MS-94

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

B.8 auto-action log MS-94

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

B.9 auto-advise IPM MS

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

B.10 auto-assignment of annotations MS-94

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

B.11 auto-assignment of group names MS–94

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

B.12 auto-assignment of storage period MS-94

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

B.13 auto-correlation of IP-messages IPM MS-94

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

1) IP-messages received in reply to, or sent in reply to an IP-message;

2) the IP-messages which forwarded (or auto-forwarded) one or more messages;

3) the received or submitted IP-messages that obsolete an IP-message;

4) the received or submitted IP-messages that indicate that they are related to an IP-message.

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

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

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

B.15 auto-correlation of reports MS-94

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

B.16 auto-deletion after storage period MS-94

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

B.17 auto-discarding of IP-messages IPM MS-94

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

B.18 auto-forwarded indication IPM

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

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

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

B.19 auto-forwarding of IP-messages IPM MS

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

NOTE – In versions of 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.

B.20 auto-submitted indication IPM

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

– not auto-submitted;

– auto-generated;

– auto-replied.

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

B.21 basic physical rendition PD PR

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

B.22 blind copy recipient indication IPM PR

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

B.23 body part authentication and integrity IPM

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

B.24 body part encryption IPM

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

B.25 circulation list recipients indication IPM

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

B.26 content confidentiality MT

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

B.27 content integrity MT PR

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

B.28 content type indication MT

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

B.29 conversion prohibition MT

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

B.30 conversion prohibition in case of loss of information MT

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

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

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

B.31 converted indication MT PR

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

B.32 counter collection PD PR

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

B.33 counter collection with advice PD PR

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

B.34 cover page suppression MT PR

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

B.35 cross-referencing indication IPM

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

B.36 deferred delivery MT

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

B.37 deferred delivery cancellation MT

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

B.38 delivery log MS-94

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

B.39 delivery notification MT PR

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

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

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

B.40 delivery time stamp indication MT PR

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

B.41 delivery via bureaufax service PD PR

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

B.42 designation of recipient by directory name MT PR

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

B.43 disclosure of other recipients MT

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

B.44 distribution codes indication IPM

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

B.45 DL-exempted recipients MT

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

B.46 DL-expansion history indication MT

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

B.47 DL-expansion prohibited MT

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

B.48 EMS (Express Mail Service) PD PR

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

B.49 expiry date indication IPM

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

B.50 explicit conversion MT PR

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

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

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

B.51 forwarded IP-message indication IPM

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

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

B.52 grade of delivery selection MT

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

B.53 hold for delivery MT

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

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

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

B.54 implicit conversion MT

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

B.55 importance indication IPM

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

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

B.56 incomplete copy indication IPM

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

B.57 information category indication IPM

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

B.58 IP-message action status IPM MS-94

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

B.59 IP-message identification IPM

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

B.60 IP-message security labelling IPM

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

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

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

B.61 language indication IPM

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

B.62 latest delivery designation MT

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

B.63 manual handling instructions indication IPM

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

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

B.64 message flow confidentiality MT

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

NOTE – Only a limited form of this is supported.

B.65 message identification MT

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

B.66 message origin authentication MT PR

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

B.67 message security labelling MT

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

B.68 message sequence integrity MT PR

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

B.69 MS register MS

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

1) the performance of automatic actions;

2) the default set of information retrieved when using the Stored Message Fetching and Stored Message Listing Elements of Service. One set of information may be registered per UA employed by the user;

3) the credentials used by the Message Store to authenticate the MS-user.

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

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

B.70 multi-destination delivery MT PR

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

B.71 multi-part body IPM

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

B.72 non-delivery notification MT PR

This element of service enables the MTS to notify an originating UA if a submitted message was not delivered to the specified recipient UA(s), 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 UAs to which the message could not be delivered.

When a message is not delivered after distribution list expansion, then, depending on the policy of the distribution list, the notification can be sent to either the list owner, the message originator, or both.

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

B.73 non-receipt notification request indication IPM PR

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

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

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

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

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

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

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

B.74 non-repudiation of content received IPM PR

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 notarization 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.

B.75 non-repudiation of delivery MT PR

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

B.76 non-repudiation of IP-notification IPM PR

This element of service provides the recipient of an 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 of ITU-T Rec. X.402 | 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.

B.77 non-repudiation of origin MT PR

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

B.78 non-repudiation of submission MT

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

B.79 obsoleting indication IPM

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

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

B.80 ordinary mail PD PR

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

B.81 original encoded information types indication MT

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

B.82 originator indication IPM

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

B.83 originator reference indication IPM

This element of service enables the originator to indicate to a recipient a reference that is chosen by the originator. The originator reference may be used within the organization of the originator as an internal reference. Examples of possible originator references include: file number, claim number and legal case number. This information may be used by the recipient in later communications with the originator, possibly via non-MHS means, concerning a particular IP-message.

B.84 originator requested alternate recipient MT PR

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

B.85 physical delivery notification by MHS PD PR

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

NOTE 1 – The notification includes the date and time of delivery based on the delivery confirmation given by the delivery person, the addressee or another authorized person. This is subject to national regulations in the destination 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.132 is overridden.

B.86 physical delivery notification by PDS PD PR

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

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

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

NOTE 3 – When this element of service is requested, and the physical message is undeliverable, 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.132 is overridden.

B.87 physical forwarding allowed PD PR

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

B.88 physical forwarding prohibited PD PR

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

B.89 precedence indication IPM PR

This element of service enables an originator to indicate a precedence value for each recipient of the message. The per-recipient precedence value provides an indication of the perceived importance of the IP-message or its expected relevance to the recipients. The aggregate of precedence values assigned to all the recipients of a message shall also affect the Grade of Delivery Selection (see B.52). Whether the UA performs multiple submissions to the MTS using different Grade of Delivery Selection values is a local matter.

The semantics of values used by this service shall be determined by local policy. The following is an example of possible precedence values:

– *deferred*: The message is of relatively low importance to the recipient, and should be handled after all other messages; this value corresponds to a Grade of Delivery selection of *non-urgent*.

– *normal*: The message is a routine communication of no distinguishing importance to the recipient, and should be handled at the convenience of the recipient; this value corresponds to a Grade of Delivery selection of *normal*.

– *action-today*: The message is of high importance to the recipient, and should be acted upon by the recipient before the close of the current business day; this value corresponds to a Grade of Delivery selection of *urgent*.

– *immediate*: The message is for the immediate attention of the recipient, and should be acted upon by the recipient with all possible speed; this value corresponds to a Grade of Delivery selection of *urgent*.

B.90 prevention of non-delivery notification MT PR

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

B.91 primary and copy recipients indication IPM

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

The names of users and DLs can be expressed in several ways, some of which are intended for human use only and not intended to be names by which the MHS could make deliveries. This element of service allows originators to distinguish between the names which the originating UA will add to the Multi-destination Delivery (see B.70) and the names to which the MHS will not be requested to make deliveries. This may result in none of the primary recipients or copy recipients contributing to the Multi-destination Delivery.

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

B.92 probe MT

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

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

B.93 probe origin authentication MT

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

B.94 proof of content received IPM PR

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 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 or Message Origin Authentication Elements 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 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 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 or on a per-recipient basis using the Message-token as defined in ITU-T Rec. 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 ITU-T Rec. X.411 | ISO/IEC 10021-4.

B.95 proof of delivery MT PR

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

B.96 proof of IP-notification IPM PR

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 Elements 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 of ITU-T Rec. X.402 | 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.

B.97 proof of submission MT

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

B.98 receipt notification request indication IPM PR

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

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

B.99 redirection disallowed by originator MT

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

B.100 redirection of incoming messages MT

This element of service enables a recipient UA, through registration, to instruct the MTS to redirect incoming messages addressed to it, to another UA or to a DL. This instruction remains in effect 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 to occur 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 different alternate recipients or not redirected at all.

B.101 registered mail PD PR

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

B.102 registered mail to addressee in person PD PR

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

B.103 reply request indication IPM PR

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

NOTE – A blind copy recipient should consider carefully to whom he sends a reply, in order that the meaning of the Blind Copy Recipient Indication Element of Service is preserved.

B.104 replying IP-message indication IPM

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

1) The recipients specified in the reply request indication of the replied-to message.

2) The originator of the replied-to message.

3) The originator and other recipients.

4) A distribution list, in which the originator of the replied-to message can be a receiving member.

5) Other recipients as chosen by the originator of the reply.

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

B.105 report origin authentication MT

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

B.106 request for forwarding address PD PR

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

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

B.107 request for non-repudiation of content received IPM PR

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.

B.108 request for non-repudiation of IP-notification IPM PR

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.

B.109 request for proof of content received IPM PR

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.

B.110 request for proof of IP-notification IPM PR

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.

B.111 requested preferred delivery method MT PR

This element of service allows a user to request, on a per-recipient basis, the preference of method or methods of message delivery (such as through an Access Unit).

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-addresses available in the Directory. Non-delivery may occur if no feasible match can be found.

B.112 restricted delivery MT

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.

The recipient UA may register several sets of criteria to restrict the delivery of different categories of message.

B.113 return of content MT

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

B.114 secure access management MT

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

B.115 sensitivity indication IPM

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

1) Whether the recipient should have to prove his identity to receive the IP-message.

2) Whether the IP-message should be allowed to be printed on a shared printer.

3) Whether an IPM UA should allow the recipient to forward the received IP-message.

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

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

If no sensitivity level is indicated, it should be assumed that the IP-message's 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.

B.116 special delivery PD PR

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.

B.117 storage of draft messages MS-94

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.

B.118 storage on submission MS-94

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.

B.119 storage period assignment MS-94

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.

B.120 stored message alert MS

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

1) If the UA is connected and on-line to the MS, the alert message will be sent to the UA as soon as a message arrives at the MS that 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.

B.121 stored message annotation MS-94

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.19 is not related to message annotations.

B.122 stored message deletion MS

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.

B.123 stored message fetching MS

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

B.124 stored message grouping MS-94

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.

B.125 stored message listing MS

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

B.126 stored message summary MS

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

B.127 subject indication IPM

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

B.128 submission log MS-94

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.

B.129 submission of IP-messages incorporating stored messages IPM MS-94

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.

B.130 submission time stamp indication MT

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

B.131 typed body IPM

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

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.

B.132 undeliverable mail with return of physical message PD PR

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

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

B.133 use of distribution list MT PR

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

B.134 user/UA capabilities registration MT

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 the 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.

ITU-T RECOMMENDATIONS SERIES

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