



INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.402

(06/1999)

SERIES X: DATA NETWORKS AND OPEN SYSTEM
COMMUNICATIONS

Message Handling Systems

Information technology – Message Handling Systems (MHS) – Overall Architecture

ITU-T Recommendation X.402

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.369
IP-based networks	X.370–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 the list of ITU-T Recommendations.

**Information technology –
Message Handling Systems (MHS) –
Overall Architecture**

Summary

This Recommendation | International Standard contains Directory Attribute and Object Class definitions, some new and the remainder revised to use the new X.500 Recommendations. The ASN.1 has been fully revised to use the new X.680 and X.880 Recommendations. Numerous defect corrections are incorporated. This Recommendation | International Standard also contains enhancements on international registration authority, use of ISO/IEC 10646 characters in OR-addresses, protected change credentials and use of 1997 Directory.

Source

The ITU-T Recommendation X.402 was approved on 18 June 1999. The identical text is also published as ISO/IEC International Standard 10021-2.

Following ITU-T decision to publish new editions of the set of Message Handling Recommendations, this edition of ITU-T Rec. X.402 consolidates X.402 (11/1995), X.402 Technical Corrigendum 1 (08/1997) and X.402 Amendment 1 (12/1997).

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. 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 turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSC Resolution 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 expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. 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, ITU [had/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.

© ITU 2003

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

CONTENTS

	<i>Page</i>
SECTION 1 – INTRODUCTION	1
1 Scope	1
2 Normative references	3
2.1 Open Systems Interconnection	3
2.2 Directory Systems	4
2.3 Message Handling Systems	4
2.4 Country Codes	5
2.5 Network Addresses	5
2.6 Language Code	5
2.7 Character Sets	5
3 Definitions	5
3.1 Open Systems Interconnection	5
3.2 Directory Systems	6
3.3 Message Handling Systems	7
4 Abbreviations	7
5 Conventions	7
5.1 ASN.1	7
5.2 Grade	7
5.3 Terms	7
SECTION 2 – ABSTRACT MODELS	8
6 Overview	8
7 Functional Model	8
7.1 Primary Functional Objects	8
7.1.1 The Message Handling System	9
7.1.2 Users	9
7.1.3 Distribution Lists	9
7.2 Secondary Functional Objects	9
7.2.1 The Message Transfer System	10
7.2.2 User Agents	10
7.2.3 Message Stores	10
7.2.4 Access Units	10
7.3 Tertiary Functional Objects	11
7.3.1 Message Transfer Agents	11
7.4 Selected AU Types	11
7.4.1 Physical Delivery	11
7.4.2 Telematic	11
7.4.3 Telex	12
8 Information Model	12
8.1 Messages	12
8.2 Probes	13
8.3 Reports	13
9 Operational Model	13
9.1 Transmittal	13
9.2 Transmittal Roles	14
9.3 Transmittal Steps	15
9.3.1 Origination	15
9.3.2 Submission	16
9.3.3 Import	16
9.3.4 Transfer	16
9.3.5 Export	16
9.3.6 Delivery	16
9.3.7 Retrieval	16
9.3.8 Receipt	17

	<i>Page</i>
9.4 Transmittal Events	17
9.4.1 Splitting	17
9.4.2 Joining	17
9.4.3 Name Resolution	18
9.4.4 DL Expansion	18
9.4.5 Redirection	18
9.4.6 Conversion	18
9.4.7 Non-delivery	18
9.4.8 Non-affirmation	18
9.4.9 Affirmation	18
9.4.10 Routing	19
10 Security Model	19
10.1 Security Policies	19
10.2 Security Services	19
10.2.1 Origin Authentication Security Services	20
10.2.2 Secure Access Management Security Service	21
10.2.3 Data Confidentiality Security Services	21
10.2.4 Data Integrity Security Services	22
10.2.5 Non-Repudiation Security Services	23
10.2.6 Message Security Labelling Security Service	23
10.2.7 Security Management Services	23
10.3 Security Elements	24
10.3.1 Authentication Security Elements	24
10.3.2 Secure Access Management Security Elements	25
10.3.3 Data Confidentiality Security Elements	26
10.3.4 Data Integrity Security Elements	26
10.3.5 Non-repudiation Security Elements	27
10.3.6 Security Label Security Elements	27
10.3.7 Security Management Security Elements	27
10.3.8 Double Enveloping Technique	27
10.3.9 Encoding for Encryption and Hashing	27
SECTION 3 – CONFIGURATIONS	27
11 Overview	27
12 Functional Configurations	28
12.1 Regarding the Directory	28
12.2 Regarding the Message Store	28
13 Physical Configurations	28
13.1 Messaging Systems	29
13.1.1 Access Systems	30
13.1.2 Storage Systems	30
13.1.3 Access and Storage Systems	30
13.1.4 Transfer Systems	30
13.1.5 Access and Transfer Systems	30
13.1.6 Storage and Transfer Systems	30
13.1.7 Access, Storage, and Transfer Systems	30
13.2 Representative Configurations	30
13.2.1 Fully Centralized	30
13.2.2 Centralized Message Transfer and Storage	31
13.2.3 Centralized Message Transfer	31
13.2.4 Fully Distributed	31
14 Organizational Configurations	31
14.1 Management Domains	31
14.1.1 Administration Management Domains	32
14.1.2 Private Management Domains	32
14.2 Representative Configurations	32
14.2.1 Fully Centralized	32
14.2.2 Directly Connected	32
14.2.3 Indirectly Connected	32

15	The Global MHS	32
SECTION 4 – NAMING, ADDRESSING, AND ROUTING		33
16	Overview	33
17	Naming	34
17.1	Directory Names	34
17.2	OR-Names	34
18	Addressing	34
18.1	Attribute Lists	35
18.2	Character Sets	35
18.3	Standard Attributes	36
18.3.1	Administration-domain-name	37
18.3.2	Common-name	37
18.3.3	Country-name	37
18.3.4	Extension-postal-OR-address-components	38
18.3.5	Extension-physical-delivery-address-components	38
18.3.6	Local-postal-attributes	38
18.3.7	Network-address	38
18.3.8	Numeric-user-identifier	38
18.3.9	Organization-name	38
18.3.10	Organizational-unit-names	39
18.3.11	Pds-name	39
18.3.12	Personal-name	39
18.3.13	Physical-delivery-country-name	39
18.3.14	Physical-delivery-office-name	39
18.3.15	Physical-delivery-office-number	39
18.3.16	Physical-delivery-organization-name	39
18.3.17	Physical-delivery-personal-name	39
18.3.18	Post-office-box-address	40
18.3.19	Postal-code	40
18.3.20	Poste-restante-address	40
18.3.21	Private-domain-name	40
18.3.22	Street-address	40
18.3.23	Terminal-identifier	40
18.3.24	Terminal-type	40
18.3.25	Unformatted-postal-address	40
18.3.26	Unique-postal-name	41
18.4	Attribute List Equivalence	41
18.5	OR-Address Forms	41
18.5.1	Mnemonic OR-Address	42
18.5.2	Numeric OR-Address	42
18.5.3	Postal OR-Address	43
18.5.4	Terminal OR-Address	43
18.5.5	Determination of Address Forms	44
18.6	Conditional Attributes	44
19	Routing	44
SECTION 5 – USE OF THE DIRECTORY		45
20	Overview	45
21	Authentication	45
22	Name Resolution	46
23	DL Expansion	46
24	Capability Assessment	46
SECTION 6 – OSI REALIZATION		47
25	Overview	47

	<i>Page</i>
26 Application Service Elements	47
26.1 The ASE Concept.....	47
26.2 Symmetric and Asymmetric ASEs.....	48
26.3 Message Handling ASEs.....	49
26.3.1 Message Transfer	49
26.3.2 Message Submission	49
26.3.3 Message Delivery.....	49
26.3.4 Message Retrieval.....	49
26.3.5 Message Administration.....	50
26.4 Supporting ASEs.....	50
26.4.1 Remote Operations.....	50
26.4.2 Reliable Transfer.....	50
26.4.3 Association Control.....	50
27 Application Contexts.....	50
SECTION 7 – ABSTRACT SERVICE DEFINITION CONVENTIONS	51
28 Overview	51
29 Components of the Abstract Model.....	51
29.1 Abstract Objects.....	51
29.2 Abstract Contracts.....	51
29.3 Connection Packages	52
29.4 Abstract Ports	52
29.5 Abstract Operations and Abstract Errors.....	52
30 ROS Realization	52
Annex A – Directory Object Classes and Attributes	54
A.1 Object Classes	54
A.1.1 MHS Distribution List.....	54
A.1.2 MHS Message Store.....	54
A.1.3 MHS Message Transfer Agent.....	54
A.1.4 MHS User	55
A.1.5 MHS User Agent.....	55
A.2 Attributes.....	55
A.2.1 MHS Acceptable EITs	55
A.2.2 MHS Deliverable Classes	56
A.2.3 MHS Deliverable Content Types	56
A.2.4 MHS DL Archive Service.....	56
A.2.5 MHS DL Members.....	56
A.2.6 MHS DL Policy	56
A.2.7 MHS DL Related Lists.....	57
A.2.8 MHS DL Submit Permissions.....	57
A.2.9 MHS DL Subscription Service.....	57
A.2.10 MHS Exclusively Acceptable EITs.....	57
A.2.11 MHS Maximum Content Length.....	57
A.2.12 MHS Message Store Directory Name	57
A.2.13 MHS OR-Addresses.....	58
A.2.14 MHS OR-Addresses with Capabilities.....	58
A.2.15 MHS Supported Attributes.....	58
A.2.16 MHS Supported Automatic Actions	58
A.2.17 MHS Supported Content Types	58
A.2.18 MHS Supported Matching Rules	59
A.2.19 MHS Unacceptable EITs.....	59
A.3 Attribute Syntaxes.....	59
A.3.1 DL Submit Permission	59
A.3.2 DL Policy	60
A.3.3 OR-Address.....	62
A.3.4 OR-Address with Capabilities.....	62
A.3.5 OR-Name	63

	<i>Page</i>
A.4 Contexts	63
A.4.1 DL Administrator Annotation	63
A.4.2 DL Nested DL	64
A.4.3 DL Reset Originator	64
A.5 Certificate Subject Alternative Names	64
A.5.1 MTA Name	64
Annex B – Reference Definition of Object Identifiers	65
Annex C – Reference Definition of Directory Object Classes and Attributes	67
Annex D – Security Threats	74
D.1 Masquerade	74
D.2 Message Sequencing	74
D.3 Modification of Information	75
D.4 Denial of Service	75
D.5 Repudiation	76
D.6 Leakage of Information	76
D.7 Other Threats	76
Annex E – Provision of Security Services in ITU-T Rec. X.411 ISO/IEC 10021-4	77
Annex F – Representation of OR-Addresses for Human Usage	78
F.1 Purpose	78
F.2 Scope	78
F.3 Format	78
F.3.1 General	78
F.3.2 Labelled format	79
F.3.3 Self-explanatory format	81
F.4 User Interface	81
Annex G – Use of OR-Addresses by Multinational Organizations	83
G.1 Addressing principles	83
G.2 Example configurations	84
G.2.1 Multiple Independent PRMDs	84
G.2.2 A single PRMD, named from a "home" country	84
G.2.3 A single PRMD with multiple country and domain names	85
G.3 Alias OR-addresses	86
Annex H – Use of Protected Passwords for Message Store Access	87
Annex I – Differences Between ISO/IEC 10021-2 and ITU-T Rec. X.402	90
Annex J – Summary of Changes to Previous Editions	91
J.1 Differences between ISO/IEC 10021-2:1990 and CCITT Rec. X.402 (1992)	91
J.2 Differences between CCITT Rec. X.402 (1992) and ITU-T Rec. X.402 (1995) ISO/IEC 10021-2:1996	91
J.3 Differences between ITU-T Rec. X.402 (1995) ISO/IEC 10021-2:1996 and ITU-T Rec. X.402 (1999) ISO/IEC 10021-2:1999	91
Annex K – Index	92

Introduction

This Specification is one of a set of Recommendations | International Standards for Message Handling. The entire set provides a comprehensive blueprint for a Message Handling System (MHS) realized by any number of cooperating open systems.

The purpose of an MHS is to enable users to exchange messages on a store-and-forward basis. A message submitted on behalf of one user, the originator, is conveyed by the Message Transfer System (MTS) and subsequently delivered to the agents of one or more additional users, the recipients. Access units (AUs) link the MTS to communication systems of other kinds (e.g., postal systems). A user is assisted in the preparation, storage, and display of messages by a user agent (UA). Optionally, he is assisted in the storage of messages by a message store (MS). The MTS comprises a number of message transfer agents (MTAs) which collectively perform the store-and-forward message transfer function.

This Specification specifies the overall architecture of the MHS and serves as a technical introduction to it.

This Specification was developed jointly by ITU-T and ISO/IEC. It is published as common text as ITU-T Rec. X.402 | ISO/IEC 10021-2.

**INTERNATIONAL STANDARD
ITU-T RECOMMENDATION**

**Information technology –
Message Handling Systems (MHS) –
Overall Architecture**

SECTION 1 – INTRODUCTION

1 Scope

This Recommendation | International Standard defines the overall architecture of the MHS and serves as a technical introduction to it.

Other aspects of Message Handling are specified in other Recommendations | parts of ISO/IEC 10021. A non-technical overview of Message Handling is provided by ITU-T Rec. X.400 | ISO/IEC 10021-1. The conformance testing of MHS components is described in Rec. X.403. The detailed rules by which the MTS converts the contents of messages from one EIT to another are defined in Rec. X.408. The abstract service the MTS provides and the procedures that govern its distributed operation are defined in ITU-T Rec. X.411 | ISO/IEC 10021-4. The abstract service the MS provides is defined in ITU-T Rec. X.413 | ISO/IEC 10021-5. The application protocols that govern the interactions of MHS components are specified in ITU-T Rec. X.419 | ISO/IEC 10021-6. The Interpersonal Messaging System, an application of Message Handling, is defined in ITU-T Rec. X.420 | ISO/IEC 10021-7. Telematic access to the Interpersonal Messaging System is specified in Rec. T.330. The EDI Messaging Service is described in CCITT Rec. F.435 | ISO/IEC 10021-8, and the EDI Messaging System, another application of Message Handling, is defined in CCITT Rec. X.435 | ISO/IEC 10021-9. The means by which messages may be routed through the MHS is specified in ISO/IEC 10021-10. Management information for MHS components is defined in the X.460-series Recommendations | ISO/IEC 11588.

The ISO/IEC International Standards and ITU-T Recommendations on Message Handling are summarized in Table 1.

Table 1 – Specifications for Message Handling Systems

ISO/IEC	ITU-T	SUBJECT MATTER
+-----+-----+-----+-----+		
+ Introduction +-----+-----+-----+-----+		
10021-1	X.400	Service and system overview
10021-2	X.402	Overall architecture
+ Various Aspects +-----+-----+-----+-----+		
-	X.408	Encoded information type conversion rules
+ Abstract Services +-----+-----+-----+-----+		
10021-4	X.411	MTS Abstract Service definition and procedures for distributed operation
10021-5	X.413	MS Abstract Service definition
+ Protocols +-----+-----+-----+-----+		
10021-6	X.419	Protocol specifications
+ Interpersonal Messaging System +-----+-----+-----+-----+		
10021-7	X.420	Interpersonal Messaging System
-	T.330	Telematic access to IPMS
+ Electronic Data Interchange Messaging System +-----+-----+-----+-----+		
10021-8	F.435	EDI Messaging Service
10021-9	X.435	EDI Messaging System
+ Routing +-----+-----+-----+-----+		
10021-10	X.412	MHS Routing
10021-11	X.404	MHS Routing: Guide for system managers
+ MHS Management +-----+-----+-----+-----+		
11588-1	X.460	Management: Model and Architecture
11588-3	X.462	Logging Information
11588-8	X.467	Message Transfer Agent Management
+-----+-----+-----+-----+		

ISO/IEC 10021-2:2003 (E)

The Directory, the principal means for disseminating communication-related information among MHS components, is defined in the X.500-series Recommendations | ISO/IEC 9594, as summarized in Table 2.

Table 2 – Specifications for Directories

ISO/IEC	ITU-T	SUBJECT MATTER
9594-1	X.500	Overview
9594-2	X.501	Models
9594-3	X.511	Abstract service definition
9594-4	X.518	Procedures for distributed operation
9594-5	X.519	Protocol specifications
9594-6	X.520	Selected attribute types
9594-7	X.521	Selected object classes
9594-8	X.509	Authentication framework
9594-9	X.525	Replication
9594-10	X.530	System Management for administration

The architectural foundation for Message Handling is provided by other Recommendations | International Standards. The OSI Reference Model is defined in ITU-T Rec. X.200 | ISO 7498. The notation for specifying the data structures of abstract services and application protocols, ASN.1, and the associated encoding rules are defined in ITU-T Rec. X.680 | ISO/IEC 8824-1, ITU-T Rec. X.681 | ISO/IEC 8824-2, ITU-T Rec. X.682 | ISO/IEC 8824-3, ITU-T Rec. X.683 | ISO/IEC 8824-4 and ITU-T Rec. X.690 | ISO/IEC 8825-1. The means for establishing and releasing associations, the ACSE, is defined in ITU-T Rec. X.217 | ISO/IEC 8649 and ITU-T Rec. X.227 | ISO 8650-1. The means for reliably conveying APDUs over associations, the RTSE, is defined in ITU-T Rec. X.218 | ISO/IEC 9066-1 and CCITT Rec. X.228 | ISO/IEC 9066-2. The means for making requests of other open systems, the ROSE, is defined in ITU-T Rec. X.880 | ISO/IEC 13712-1, ITU-T Rec. X.881 | ISO/IEC 13712-2 and ITU-T Rec. X.882 | ISO/IEC 13712-3.

The ISO/IEC International Standards and ITU-T Recommendations which form the foundation for Message Handling are summarized in Table 3.

Table 3 – Specifications for MHS Foundations

ISO/IEC	ITU-T	SUBJECT MATTER
Model		
7498-1	X.200	OSI Reference Model
ASN.1		
8824-1	X.680	Abstract syntax notation
8824-2	X.681	ASN.1 Information Objects
8824-3	X.682	ASN.1 Constraint Specification
8824-4	X.683	ASN.1 Parameterization
8825-1	X.690	Basic encoding rules
Association Control		
8649	X.217	Service definition
8650	X.227	Protocol specification
Reliable Transfer		
9066-1	X.218	Service definition
9066-2	X.228	Protocol specification
Remote Operations		
13712-1	X.880	Concepts, Model and Notation
13712-2	X.881	Service definition
13712-3	X.882	Protocol specification

This Recommendation | International Standard is structured as follows. Section one gives a general overview. Section two presents abstract models of Message Handling. Section three specifies how one can configure the MHS to satisfy any of a variety of functional, physical, and organizational requirements. Section four describes the naming and addressing of users and distribution lists and the routing of information objects to them. Section five describes the uses the MHS may make of the Directory. Section six describes how the MHS is realized by means of OSI. The conventions used in the definition of the abstract services provided by MHS components are defined in Section seven. Annexes provide important supplemental information.

No requirements for conformance to this Recommendation | International Standard are imposed.

2 Normative references

The following Recommendations and International Standards contain provisions which, through reference in this text, constitute provisions of this Recommendation | International Standard. At the time of publication, the editions indicated were valid. All Recommendations and Standards are subject to revision, and parties to agreements based on this Recommendation | International Standard are encouraged to investigate the possibility of applying the most recent editions of the Recommendations and Standards listed below. Members of ISO and IEC maintain registers of currently valid International Standards. The Telecommunication Standardization Bureau of ITU maintains a list of currently valid ITU-T Recommendations.

2.1 Open Systems Interconnection

This Specification and others in the set cite the following OSI specifications:

- ITU-T Recommendation X.200 (1994) | ISO/IEC 7498-1:1994, *Information technology – Open Systems Interconnection – Basic Reference Model: The basic model*.
- CCITT Recommendation X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.
ISO 7498-2:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture*.
- ITU-T Recommendation X.216 (1994) | ISO/IEC 8822:1994, *Information technology – Open Systems Interconnection – Connection-oriented presentation service definition*.
- ITU-T Recommendation X.217 (1995) | ISO/IEC 8649:1996, *Information technology – Open Systems Interconnection – Service Definition for the Association Control Service Element*.
- ITU-T Recommendation X.218 (1993), *Reliable Transfer: Model and service definition*.
ISO/IEC 9066-1:1989, *Information processing systems – Text communication – Reliable Transfer – Part 1: Model and service definition*.
- ITU-T Recommendation X.227 (1995), | ISO/IEC 8650-1:1996, *Information technology – Open Systems Interconnection – Connection-oriented protocol for the Association Control Service Element: Protocol specification*.
- CCITT Recommendation X.228 (1988), *Reliable Transfer: Protocol specification*.
ISO/IEC 9066-2:1989, *Information processing systems – Text communication – Reliable Transfer – Part 2: Protocol specification*.
- ITU-T Recommendation X.666 (1997) | ISO/IEC 9834-7:1998, *Information technology – Open Systems Interconnection – Procedures for the operation of OSI Registration Authorities: Assignment of international names for use in specific contexts*.
- ITU-T Recommendation X.680 (1997) | ISO/IEC 8824-1:1998, *Information technology – Abstract Syntax Notation One (ASN.1) – Specification of Basic Notation*.
- ITU-T Recommendation X.681 (1997) | ISO/IEC 8824-2:1998, *Information technology – Abstract Syntax Notation One (ASN.1) – Information Object Specification*.
- ITU-T Recommendation X.682 (1997) | ISO/IEC 8824-3:1998, *Information technology – Abstract Syntax Notation One (ASN.1) – Constraint Specification*.
- ITU-T Recommendation X.683 (1997) | ISO/IEC 8824-4:1998, *Information technology – Abstract Syntax Notation One (ASN.1) – Parameterization of ASN.1 Specifications*.
- ITU-T Recommendation X.690 (1997) | ISO/IEC 8825-1:1998, *Information technology – ASN.1 Encoding Rules – Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*.
- ITU-T Recommendation X.880 (1994) | ISO/IEC 13712-1:1995, *Information technology – Remote Operations – Concepts, Model and Notation*.
- ITU-T Recommendation X.881 (1994) | ISO/IEC 13712-2:1995, *Information technology – Remote Operations – OSI Realisations: Remote Operations Service Element (ROSE) Service Definition*.
- ITU-T Recommendation X.882 (1994) | ISO/IEC 13712-3:1995, *Information technology – Remote Operations – OSI Realisations: Remote Operations Service Element (ROSE) Protocol Specification*.

2.2 Directory Systems

This Specification and others in the set cite the following Directory System specifications:

- ITU-T Recommendation X.500 (1997) | ISO/IEC 9594-1:1998, *Information technology – Open Systems Interconnection – The Directory – Overview of concepts, models, and services.*
- ITU-T Recommendation X.501 (1997) | ISO/IEC 9594-2:1998, *Information technology – Open Systems Interconnection – The Directory – Models.*
- ITU-T Recommendation X.509 (1997) | ISO/IEC 9594-8:1998, *Information technology – Open Systems Interconnection – The Directory – Authentication framework.*
- ITU-T Recommendation X.511 (1997) | ISO/IEC 9594-3:1998, *Information technology – Open Systems Interconnection – The Directory – Abstract service definition.*
- ITU-T Recommendation X.518 (1997) | ISO/IEC 9594-4:1998, *Information technology – Open Systems Interconnection – The Directory – Procedures for distributed operation.*
- ITU-T Recommendation X.519 (1997) | ISO/IEC 9594-5:1998, *Information technology – Open Systems Interconnection – The Directory – Protocol specifications.*
- ITU-T Recommendation X.520 (1997) | ISO/IEC 9594-6:1998, *Information technology – Open Systems Interconnection – The Directory – Selected attribute types.*
- ITU-T Recommendation X.521 (1997) | ISO/IEC 9594-7:1998, *Information technology – Open Systems Interconnection – The Directory – Selected object classes.*
- ITU-T Recommendation X.525 (1997) | ISO/IEC 9594-9:1998, *Information technology – Open Systems Interconnection – The Directory – Replication.*
- ITU-T Recommendation X.530 (1997) | ISO/IEC 9594-10:1998, *Information Technology – Open Systems Interconnection – The Directory: Use of systems management for administration of the Directory.*

2.3 Message Handling Systems

This Specification and others in the set cite the following Message Handling System specifications:

- CCITT Recommendation T.330 (1988), *Telematic access to interpersonal messaging system.*
- ITU-T Recommendation F.400/X.400 (1999), *Message handling: System and service overview.*
ISO/IEC 10021-1:1999, *Information technology – Message Handling Systems (MHS) – Part 1: System and service overview.*
- CCITT Recommendation X.408 (1988), *Message handling systems: Encoded information type conversion rules.*
- ITU-T Recommendation X.411 (1999) | ISO/IEC 10021-4:1999, *Information technology – Message Handling Systems (MHS) – Message transfer system : Abstract service definition and procedures.*
- ITU-T Recommendation X.413 (1999) | ISO/IEC 10021-5:1999, *Information technology – Message Handling Systems (MHS) – Message store: Abstract service definition.*
- ITU-T Recommendation X.419 (1999) | ISO/IEC 10021-6:1999, *Information technology – Message Handling Systems (MHS) – Protocol specifications.*
- ITU-T Recommendation X.420 (1999) | ISO/IEC 10021-7:1999, *Information technology – Message Handling Systems (MHS) – Interpersonal messaging system.*
- ITU-T Recommendation F.435 (1999), *Message handling: Electronic Data Interchange Messaging Service.*
ISO/IEC 10021-8:1999, *Information technology – Message Handling Systems (MHS) – Part 8: Electronic Data Interchange Messaging Service.*
- ITU-T Recommendation X.435 (1999) | ISO/IEC 10021-9:1999, *Information technology – Message Handling Systems (MHS) – Electronic Data Interchange Messaging System.*
- ITU-T Recommendation X.412 (1999) | ISO/IEC 10021-10:1999, *Information technology – Message Handling Systems (MHS) – MHS Routing.*
- ITU-T Recommendation X.404 (1999) | ISO/IEC TR 10021-11:1999, *Information technology – Message Handling Systems (MHS) – MHS Routing: Guide for Messaging System Managers.*
- ITU-T Recommendation X.460 (1995) | ISO/IEC 11588-1:1996, *Information technology – Message Handling Systems (MHS) Management – Model and Architecture.*

- ITU-T Recommendation X.462 (1996) | ISO/IEC 11588-3:1997, *Information technology – Message Handling Systems (MHS) Management – Logging Information.*
- ITU-T Recommendation X.467 (1996) | ISO/IEC 11588-8:1997, *Information technology – Message Handling Systems (MHS) Management – Message Transfer Agent Management.*

2.4 Country Codes

This Specification cites the following Country Code specifications:

- ISO 3166-1:1997, *Codes for the representation of names of countries and their subdivisions – Part 1: Country codes.*
- ITU-T Recommendation X.121 (1996), *International numbering plan for public data networks.*

2.5 Network Addresses

This Specification cites the following Network Address specification:

- CCITT Recommendation E.164 (1991), *Numbering plan for the ISDN era.*

2.6 Language Code

This Specification cites the following Language Code specification:

- ISO 639:1988, *Code for the representation of names of languages.*

2.7 Character Sets

This Specification cites the following Character Set specifications:

- ISO 10646-1:1993, *Information technology – Universal Multiple-Octet Coded Character Set (UCS) – Part 1: Architecture and Basic Multilingual Plane.*

3 Definitions

For the purposes of this Specification and others in the set, the following definitions apply.

3.1 Open Systems Interconnection

This Specification and others in the set make use of the following terms defined in ITU-T Rec. X.200 | ISO/IEC 7498-1, as well as the names of the seven layers of the Reference Model:

- a) abstract syntax;
- b) application entity (AE);
- c) application process;
- d) application protocol data unit (APDU);
- e) application service element (ASE);
- f) distributed information processing task;
- g) layer;
- h) open system;
- i) Open Systems Interconnection (OSI);
- j) peer;
- k) presentation context;
- l) protocol;
- m) Reference Model;
- n) transfer syntax; and
- o) user element (UE).

ISO/IEC 10021-2:2003 (E)

This Specification and others in the set make use of the following terms defined in ITU-T Rec. X.680 | ISO/IEC 8824-1, ITU-T Rec. X.681 | ISO/IEC 8824-2, ITU-T Rec. X.682 | ISO/IEC 8824-3 and ITU-T Rec. X.683 | ISO/IEC 8824-4, as well as the names of ASN.1 data types and values:

- a) Abstract Syntax Notation One (ASN.1);
- b) Basic Encoding Rules;
- c) explicit;
- d) export;
- e) implicit;
- f) import;
- g) information object class;
- h) module;
- i) tag;
- j) type; and
- k) value.

This Specification and others in the set make use of the following terms defined in ITU-T Rec. X.217 | ISO/IEC 8649:

- a) application association; association;
- b) application context (AC);
- c) Association Control Service Element (ACSE);
- d) initiator; and
- e) responder.

This Specification and others in the set make use of the following terms defined in ITU-T Rec. X.218 | ISO/IEC 9066-1:

- a) Reliable Transfer (RT); and
- b) Reliable Transfer Service Element (RTSE).

This Specification and others in the set make use of the following terms defined in ITU-T Rec. X.880 | ISO/IEC 13712-1:

- a) argument;
- b) asynchronous;
- c) bind;
- d) parameter;
- e) remote error;
- f) remote operation;
- g) Remote Operations (RO);
- h) Remote Operations Service Element (ROSE);
- i) result;
- j) synchronous; and
- k) unbind.

3.2 Directory Systems

This Specification and others in the set make use of the following terms defined in the X.500-series Recs. | ISO/IEC 9594:

- a) attribute;
- b) certificate;
- c) certification authority;
- d) certification path;
- e) directory entry; entry;
- f) directory system agent (DSA);
- g) Directory;

- h) hash function;
- i) name;
- j) object class;
- k) object;
- l) simple authentication; and
- m) strong authentication.

3.3 Message Handling Systems

For the purposes of this Specification the terms indexed in annex K apply.

4 Abbreviations

For the purposes of this Specification the abbreviations indexed in annex K apply.

5 Conventions

This Specification uses the descriptive conventions identified below.

5.1 ASN.1

This Specification uses several ASN.1-based descriptive conventions in annexes A and C to define the Message Handling-specific information the Directory may hold. ASN.1 is defined in ITU-T Rec. X.680 | ISO/IEC 8824-1, ITU-T Rec. X.681 | ISO/IEC 8824-2, ITU-T Rec. X.682 | ISO/IEC 8824-3 and ITU-T Rec. X.683 | ISO/IEC 8824-4. In particular, this Specification uses the OBJECT-CLASS and ATTRIBUTE information object classes of ITU-T Rec. X.501 | ISO/IEC 9594-2 to define Message Handling-specific object classes and attributes.

ASN.1 appears both in annex A to aid the exposition, and again, largely redundantly, in Annex C for reference. If differences are found between the two, a specification error is indicated.

ASN.1 tags are implicit throughout the ASN.1 module that Annex C defines; the module is definitive in that respect.

Although the abstract syntax in this Service Definition contains extension markers, it has not been verified that these are present in all instances that would be required before Packed Encoding Rules could safely be used.

5.2 Grade

Whenever this Specification describes a class of data structure (e.g., OR-addresses) having components (e.g., attributes), each component is assigned one of the following grades:

- a) mandatory (M): A mandatory component shall be present in every instance of the class.
- b) optional (O): An optional component shall be present in an instance of the class at the discretion of the object (e.g., user) supplying that instance. There is no default value.
- c) defaultable (D): A defaultable component shall be present in an instance of the class at the discretion of the object (e.g., user) supplying that instance. In its absence a default value, specified by this Specification, applies.
- d) conditional (C): A conditional component shall be present in an instance of the class under circumstances prescribed by this Specification.

5.3 Terms

Throughout the remainder of this Specification, terms are rendered in bold when defined, in *italic* when referenced prior to their definitions, without emphasis upon other occasions.

Terms that are proper nouns are capitalized, generic terms are not.

SECTION 2 – ABSTRACT MODELS

6 Overview

This section presents abstract models of *Message Handling* which provide the architectural basis for the more detailed specifications that appear in other MHS Specifications.

Message Handling is a distributed information processing task that integrates the following intrinsically related sub-tasks:

- a) Message Transfer: The non-real-time carriage of information objects between parties using computers as intermediaries.
- b) Message Storage: The automatic storage for later retrieval of information objects conveyed by means of Message Transfer.

This section covers the following topics:

- a) Functional model;
- b) Information model;
- c) Operational model;
- d) Security model.

NOTE – Message Handling has a variety of applications, one of which is Interpersonal Messaging, described in ITU-T Rec. X.420 | ISO/IEC 10021-7.

7 Functional Model

This clause provides a functional model of Message Handling. The concrete realization of the model is the subject of other MHS Specifications.

The Message Handling Environment (MHE) comprises "primary" functional objects of several types, the *Message Handling System (MHS)*, *users*, and *distribution lists*. The MHS in turn can be decomposed into lesser, "secondary" functional objects of several types, the *Message Transfer System (MTS)*, *user agents*, *message stores*, and *access units*. The MTS in turn can be decomposed into still lesser, "tertiary" functional objects of a single type, *message transfer agents*.

The primary, secondary, and tertiary functional object types and selected *access unit* types are individually defined and described below.

As detailed below, functional objects are sometimes tailored to one or more applications of Message Handling, e.g., Interpersonal Messaging (see ITU-T Rec. X.420 | ISO/IEC 10021-7 and CCITT Rec. T.330). A functional object that has been tailored to an application understands the syntax and semantics of the contents of messages exchanged in that application.

As a local matter, functional objects may have capabilities beyond those specified in this Specification or other MHS Specifications. In particular, a typical *user agent* has message preparation, rendition, and storage capabilities that are not standardized.

7.1 Primary Functional Objects

The MHE comprises the *Message Handling System*, *users*, and *distribution lists*. These primary functional objects interact with one another. Their types are defined and described below.

The situation is depicted in Figure 1.

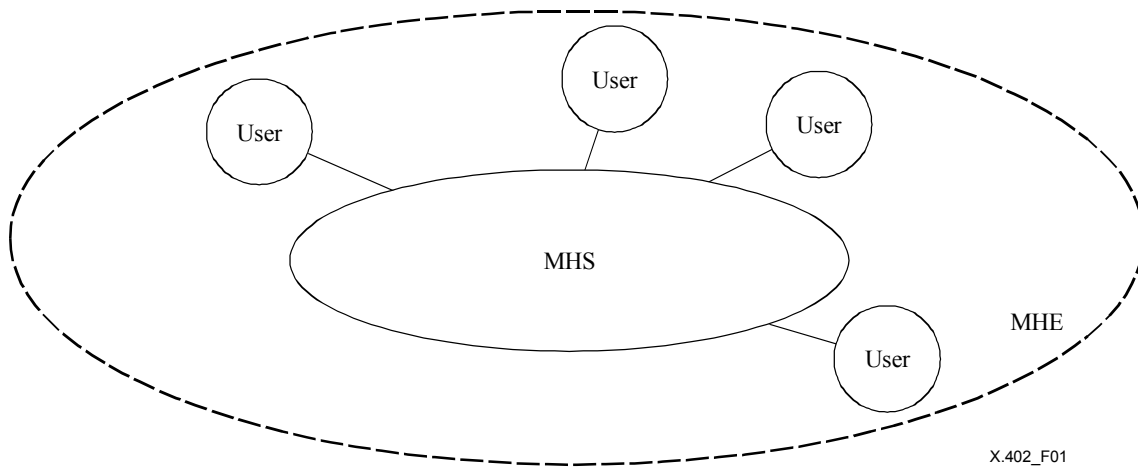


Figure 1 – The Message Handling Environment

7.1.1 The Message Handling System

The principal purpose of Message Handling is to convey information objects from one party to another. The functional object by means of which this is accomplished is called the Message Handling System (MHS).

The MHE comprises a single MHS.

7.1.2 Users

The principal purpose of the MHS is to convey information objects between *users*. A functional object (e.g., a person) that engages in (rather than provides) Message Handling is called a user.

The following kinds of user are distinguished:

- a) direct user: A user that engages in Message Handling by direct use of the MHS.
- b) indirect user: A user that engages in Message Handling by indirect use of the MHS, i.e., through another communication system (e.g., a postal system or the telex network) to which the MHS is linked.

The MHE comprises any number of users.

7.1.3 Distribution Lists

By means of the MHS a user can convey information objects to pre-specified groups of users as well as to individual users. The functional object that represents a pre-specified group of users and other *DLs* is called a distribution list (DL).

A DL identifies zero or more users and DLs called its members. The latter DLs (if any) are said to be nested. Asking the MHS to convey an information object (e.g., a *message*) to a DL is tantamount to asking that it convey the object to its members. Note that this is recursive.

The right, or permission, to convey *messages* to a particular DL may be controlled. This right is called submit permission. As a local matter the use of a DL can be further restricted.

The MHE comprises any number of DLs.

NOTE – A DL might be further restricted, e.g., to the conveyance of *messages* of a prescribed *content type*.

7.2 Secondary Functional Objects

The MHS comprises the *Message Transfer System*, *user agents*, *message stores*, and *access units*. These secondary functional objects interact with one another. Their types are defined and described below.

The situation is depicted in Figure 2.

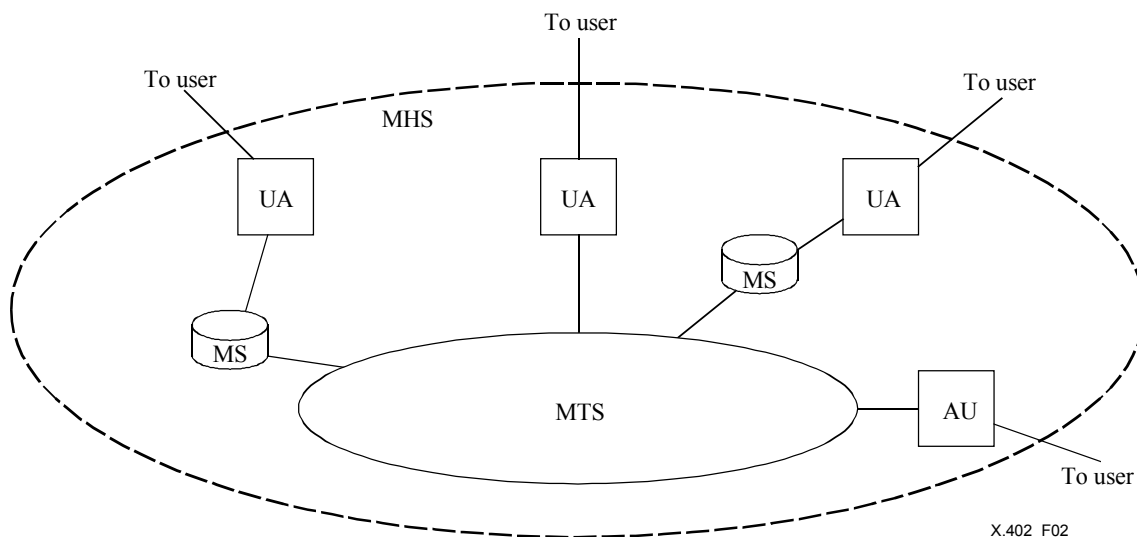


Figure 2 – The Message Handling System

7.2.1 The Message Transfer System

The MHS conveys information objects to individual users and to the members of DLs. The functional object that actually does this is called the Message Transfer System (MTS). The MTS is a store-and-forward communication system and can be considered the backbone of the MHS.

The MTS is general-purpose, supporting all applications of Message Handling. Additionally, the MTS may be tailored to one or more particular applications so it can carry out *conversion*.

The MHS comprises a single MTS.

7.2.2 User Agents

The functional object by means of which a single direct user engages in Message Handling is called a user agent (UA).

A typical UA is tailored to one or more particular applications of Message Handling.

The MHS comprises any number of UAs.

NOTE – A UA that serves a human user typically interacts with him by means of input/output devices (e.g., a keyboard, display, scanner, printer, or combination of these).

7.2.3 Message Stores

A typical user must store the information objects it receives. The functional object that provides a (single) direct user with capabilities for Message Storage is called a message store (MS). Each MS is associated with one UA, but not every UA has an associated MS.

Every MS is general-purpose, supporting all applications of Message Handling. Additionally, an MS may be tailored to one or more particular applications so that it can more capably *submit* and support the *retrieval* of *messages* associated with that application.

The MHS comprises any number of MSs.

NOTE – As a local matter a UA may provide for information objects storage that either supplements or replaces that of an MS.

7.2.4 Access Units

The functional object that links another communication system (e.g., a postal system or the telex network) to the MTS and via which its patrons engage in Message Handling as indirect users is called an access unit (AU).

A typical AU is tailored to a particular communication system and to one or more particular applications of Message Handling.

The MHS comprises any number of AUs.

7.3 Tertiary Functional Objects

The MTS comprises *message transfer agents*. These tertiary functional objects interact. Their type is defined and described below.

The situation is depicted in Figure 3.

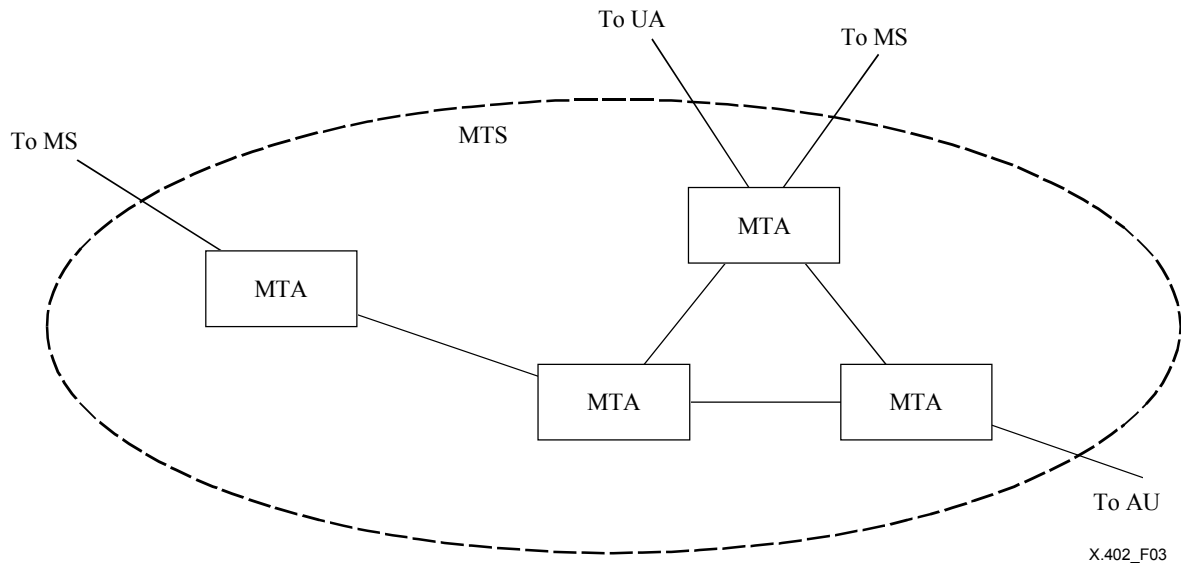


Figure 3 – The Message Transfer System

7.3.1 Message Transfer Agents

The MTS conveys information objects to users and DLs in a store-and-forward manner. A functional object that provides one link in the MTS' store-and-forward chain is called a message transfer agent (MTA).

Every MTA is general-purpose, supporting all applications of Message Handling. Additionally, an MTA may be tailored to one or more particular applications so it can carry out *conversion*.

The MTS comprises any number of MTAs.

7.4 Selected AU Types

As described above, the MHS interworks with communication systems of other types via AUs. Several selected AU types--*physical delivery*, *telematic*, and *telex*--are introduced in the subclauses below.

7.4.1 Physical Delivery

A physical delivery access unit (PDAU) is an AU that subjects *messages* (but neither *probes* nor *reports*) to *physical rendition* and that conveys the resulting *physical messages* to a *physical delivery system*.

The transformation of a *messages* into a *physical message* is called physical rendition. A physical message is a physical object (e.g., a letter and its paper envelope) that embodies a *message*.

A physical delivery system (PDS) is a system that performs *physical delivery*. One important kind of PDS is postal systems. Physical delivery is the conveyance of a physical message to a patron of a PDS, one of the indirect users to which the PDAU provides Message Handling capabilities.

Among the applications of Message Handling supported by every PDAU is Interpersonal Messaging (see ITU-T Rec. X.420 | ISO/IEC 10021-7).

7.4.2 Telematic

Telematic access units, which support Interpersonal Messaging exclusively, are introduced in ITU-T Rec. X.420 | ISO/IEC 10021-7.

7.4.3 Telex

Telex access units, which support Interpersonal Messaging exclusively, are introduced in ITU-T Rec. X.420 | ISO/IEC 10021-7.

8 Information Model

This clause provides an information model of Message Handling. The concrete realization of the model is the subject of other MHS Specifications.

The MHS and MTS can convey information objects of three classes: *messages*, *probes*, and *reports*. These classes are listed in the first column of Table 4. For each listed class, the second column indicates the kinds of functional objects--users, UAs, MSs, MTAs, and AUs--that are the ultimate sources and destinations for such objects.

Table 4 – Conveyable Information Objects

Infor- mation Object	Functional Object				
	user	UA	MS	MTA	AU
message	SD	-	-	-	-
probe	S	-	-	D	-
report	D	-	-	S	-

+- Legend -

S ultimate source

D ultimate destination

The information objects, summarized in the table, are individually defined and described in the subclauses below.

8.1 Messages

The primary purpose of Message Transfer is to convey information objects called messages from one user to others. A message has the following parts, as depicted in Figure 4:

- a) envelope: An information object whose composition varies from one *transmittal step* to another and that variously identifies the message's *originator* and *potential recipients*, documents its previous conveyance and directs its subsequent conveyance by the MTS, and characterizes its *content*.
- b) content: An information object that the MTS neither examines nor modifies, except for *conversion*, during its conveyance of the message.

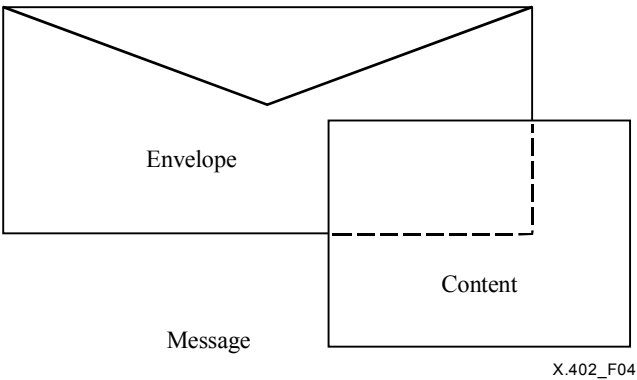


Figure 4 – A Message's Envelope and Content

One piece of information borne by the envelope identifies the type of the content. The content type is an identifier (an ASN.1 Object Identifier or Integer) that denotes the syntax and semantics of the content overall. This identifier

enables the MTS to determine the message's *deliverability* to particular users, and enables UAs and MSs to interpret and process the content.

Another piece of information borne by the envelope identifies the types of encoded information represented in the content. An encoded information type (EIT) is an identifier that denotes the medium and format (e.g., IA5 text or Group 3 facsimile) of individual portions of the content. It further enables the MTS to determine the message's deliverability to particular users, and to identify opportunities for it to *make* the message deliverable by converting a portion of the content from one EIT to another.

8.2 Probes

A second purpose of Message Transfer is to convey information objects called probes from one user up to but just short of other users (i.e., to the MTAs serving those users). A probe describes a class of message and is used to determine the *deliverability* of such messages.

A message described by a probe is called a described message.

A probe comprises an envelope alone. This envelope contains much the same information as that for a message. Besides bearing the content type and encoded information types of a described message, the probe's envelope bears the length of its content.

The *submission* of a probe elicits from the MTS largely the same behaviour as would submission of any described message, except that *DL expansion* and *delivery* are forgone in the case of the probe. In particular, and apart from the consequences of the suppression of *DL expansion*, the probe provokes the same *reports* as would any described message. This fact gives probes their utility.

8.3 Reports

A third purpose of Message Transfer is to convey information objects called reports to users. Generated by the MTS, a report relates the outcome or progress of a message's or probe's *transmittal* to one or more *potential recipients*.

The message or probe that is the subject of a report is called its subject message or subject probe.

A report concerning a particular *potential recipient* is conveyed to the originator of the subject message or probe unless the *potential recipient* is a *member recipient*. In the latter case, the report is conveyed to the DL of which the *member recipient* is a member. As a local matter (i.e., by policy established for that particular DL), the report may be further conveyed to the DL's owner; either to the containing DL (in the case of nesting) or to the originator of the subject message (otherwise); or both.

The outcomes that a single report may relate are of the following kinds:

- a) delivery report: *Delivery*, *exports*, or a *affirmation* of the subject message or probe, or *DL expansion*.
- b) non-delivery report: *Non-Delivery* or *non-affirmation* of the subject message or probe.

A report may comprise one or more delivery and/or non-delivery reports. A message or probe may provoke several delivery and/or non-delivery reports concerning a particular *potential recipient*. Each marks the passage of a different transmittal *step* or *event*.

9 Operational Model

This clause provides an operational model of Message Handling. The concrete realization of the model is the subject of other MHS Specifications.

The MHS can convey an information object to individual users, DLs, or a mix of the two. Such conveyance is accomplished by a process called *transmittal* comprising *step* and *event*. The process, its parts, and the roles that users and DLs play in it are defined and described below.

9.1 Transmittal

The conveyance or attempted conveyance of a message or probe is called transmittal. Transmittal encompasses a message's conveyance from its *originator* to its *potential recipients*, and a probe's conveyance from its *originator* to MTAs able to *affirm* the described messages' *deliverability* to the probe's potential recipients. Transmittal also encompasses the conveyance or attempted conveyance to the *originator* of any reports the message or probe may provoke.

A transmittal comprises a sequence of *transmittal steps* and *events*. A transmittal step (or step) is the conveyance of a message, probe, or report from one functional object to another "adjacent" to it. A transmittal event (or event) is processing of a message, probe, or report within a functional object that may influence the functional object's selection of the next transmittal step or event.

The information flow of transmittal is depicted in Figure 5. The figure shows the kinds of functional objects--direct users, indirect users, UAs, MSs, MTAs, and AUs--that may be involved in a transmittal, the information objects--messages, probes, and reports--that may be conveyed between them, and the names of the transmittal steps by means of which those conveyances are accomplished.

The figure highlights the facts that a message or report may be retrieved repeatedly and that only the first conveyance of a retrieved object from UA to user constitutes *receipt*.

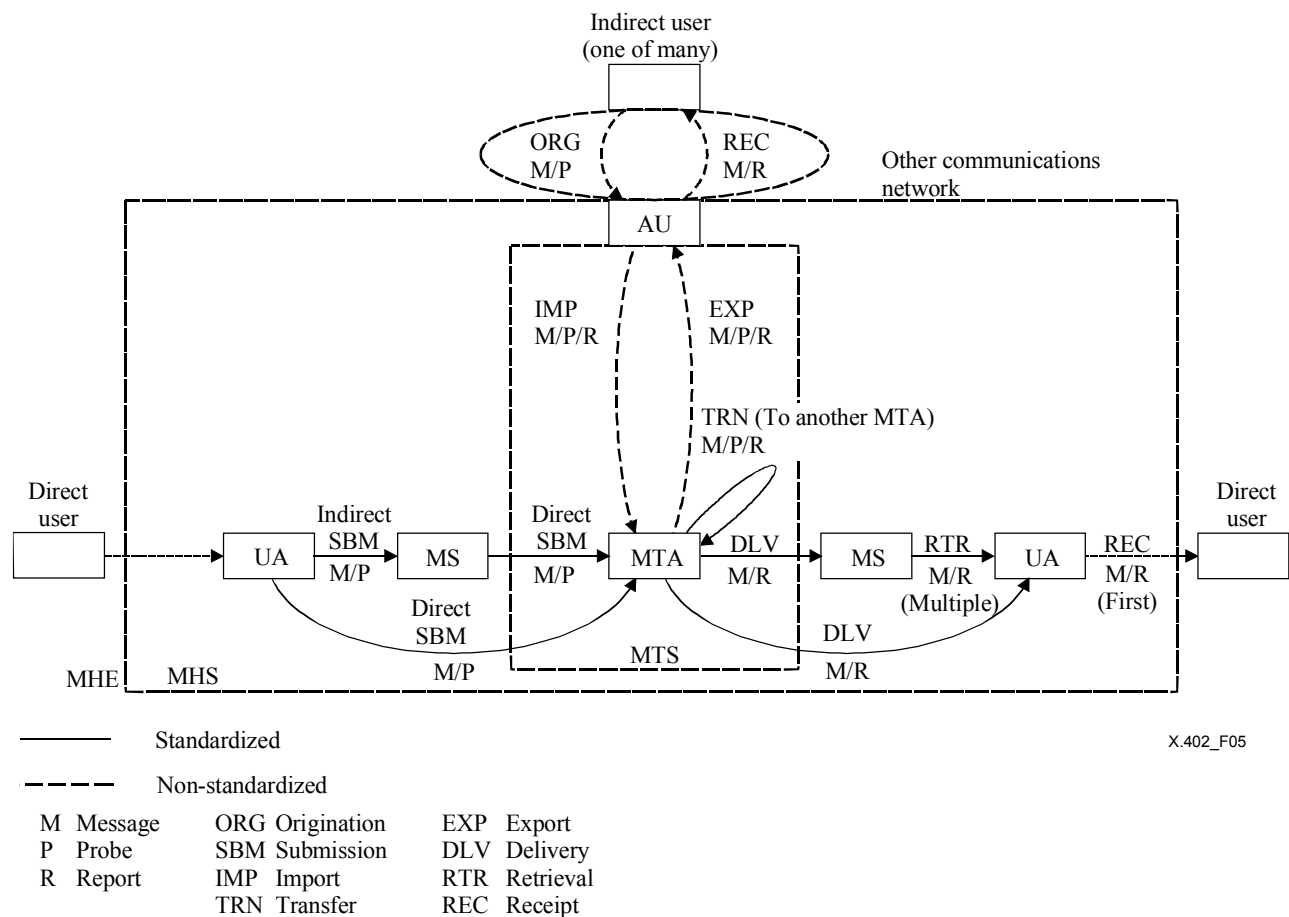


Figure 5 – The information flow of transmittal

One event plays a distinguished role in transmittal. *Splitting* replicates a message or probe and divides responsibility for its immediate recipients among the resulting information objects. The potential recipients associated with a particular instance of a message or probe are called the immediate recipients. An MTA stages a splitting if the next step or event required in the conveyance of a message or probe to some immediate recipients differs from that required in its conveyance to others. Each of the step and event descriptions which follow assumes that the step or event is appropriate for all immediate recipients, a situation that can be created, if necessary, by splitting.

9.2 Transmittal Roles

Users and DLs play a variety of roles in a message's or probe's transmittal. These roles are informally categorized as "source" roles, "destination" roles, or statuses to which users or DLs can be elevated.

A user may play the following "source" role in the transmittal of a message or probe:

- originator: The user (but not DL) that is the ultimate source of a message or probe.

A user or DL may play any of the following "destination" roles in the transmittal of a message or probe:

- a) intended recipient: One of the users and DLs the originator specifies as a message's or probe's intended destinations.
- b) originator-specified alternate recipient: The user or DL (if any) to which the originator requests that a message or probe be conveyed if it cannot be conveyed to a particular intended recipient.
- c) member recipient: A user or DL to which a message (but not a probe) is conveyed as a result of *DL expansion*.
- d) recipient-assigned alternate recipient: The user or DL (if any) to which an intended, originator-specified alternate, or member recipient may have elected to *redirect* messages.

A user or DL may attain any of the following statuses in the course of a message's or probe's transmittal:

- a) potential recipient: Any user or DL to (i.e., toward) which a message or probe is conveyed at any point during the course of transmittal. Necessarily an intended, originator-specified alternate, member, or recipient-assigned alternate recipient.
- b) actual recipient (or recipient): A potential recipient for which *delivery* or *affirmation* takes place.

9.3 Transmittal Steps

The kinds of steps that may occur in a transmittal are listed in the first column of Table 5. For each listed kind, the second column indicates whether such steps are standardized, the third column the kinds of information objects--messages, probes, and reports--that may be conveyed in such a step, the fourth column the kinds of functional objects--users, UAs, MSs, MTAs, and AUs--that may participate in such a step as the object's source or destination.

The table is divided into three sections. The steps in the first section apply to the "creation" of messages and probes, those in the last to the "disposal" of messages and reports, and those in the middle section to the "relaying" of messages, probes, and reports.

Table 5 – Transmittal Steps

Transmittal Step	Stand- ard- ized?	Information Objects			Functional Objects				
		M	P	R	user	UA	MS	MTA	AU
origination	No	x	x	-	S	D	-	-	-
submission	Yes	x	x	-	-	S	SD	D	-
import	No	x	x	x	-	-	-	D	S
transfer	Yes	x	x	x	-	-	-	SD	-
export	No	x	x	x	-	-	-	S	D
delivery	Yes	x	-	x	-	D	D	S	-
retrieval	Yes	x	-	x	-	D	S	-	-
receipt	No	x	-	x	D	S	-	-	-

Legend		
M message	S source	x permitted
P probe	D destination	
R report		

The kinds of transmittal steps, summarized in the table, are individually defined and described in the subclauses below.

9.3.1 Origination

In an origination step, either a direct user conveys a message or probe to its UA, or an indirect user conveys a message or probe to the communication system that serves it. This step gives birth to the message or probe and is the first step in its transmittal.

The user above constitutes the message's or probe's originator. In this step, the originator identifies the message's or probe's intended recipients. Additionally, for each intended recipient, the originator may (but need not) identify an originator-specified alternate recipient.

9.3.2 Submission

In a submission step, a message or probe is conveyed to an MTA and thus entrusted to the MTS. Two kinds of submission are distinguished:

- a) indirect submission: A transmittal step in which the originator's UA conveys a message or probe to its MS and in which the MS effects *direct submission*. Such a step follows origination.

This step may be taken only if the user is equipped with an MS.

- b) direct submission: A transmittal step in which the originator's UA or MS conveys a message or probe to an MTA. Such a step follows origination or occurs as part of indirect submission.

This step may be taken whether or not the user is equipped with an MS.

Indirect and direct submission are functionally equivalent except that additional capabilities may be available with the former. Indirect submission may differ from direct submission in other respects (e.g., the number of open systems with which that embodying a UA must interact) and for that reason be preferable to direct submission.

The UA or MS involved in direct submission is called the submission agent. A submission agent is made known to the MTS by a process of registration, as a result of which the submission agent and MTS keep one another informed of their names, their locations, and any other characteristics required for their interaction.

9.3.3 Import

In an import step, an AU conveys a message, probe, or report to an MTA. This step injects into the MTS an information object born in another communication system, and follows its conveyance by that system.

NOTE – The concept of importing is a generic one. How this step is effected varies, of course, from one type of AU to another.

9.3.4 Transfer

In a transfer step, one MTA conveys a message, probe, or report to another. This step transports an information object over physical and sometimes organizational distances and follows direct submission, import, or (a prior) transfer.

This step may be taken, of course, only if the MTS comprises several MTAs.

The following kinds of transfer are distinguished, on the basis of the number of *MDs* involved:

- a) internal transfer: A transfer involving MTAs within a single *MD*.
- b) external transfer: A transfer involving MTAs in different *MDs*.

9.3.5 Export

In an export step, an MTA conveys a message, probe, or report to an AU. This step ejects from the MTS an information object bound for another communication system. It follows direct submission, import, or transfer.

As part of this step, the MTA may generate a delivery report. Depending on the requirements for the type of access unit defined in the relevant Message Handling specifications, a positive delivery report indicates either successful acceptance of the message (or probe) by the access unit, or that the access unit has successfully performed further conveyance of the message (or probe).

NOTE – The concept of exporting is a generic one. How this step is effected varies, of course, from one type of AU to another.

9.3.6 Delivery

In a delivery step, an MTA conveys a message or report to an MS or UA. The MS and UA are those of a potential recipient of the message, or the originator of the report's subject message or probe. This step entrusts the information object to a representative of the user and follows direct submission, import, or transfer. It also elevates the user in question to the status of an actual recipient.

As part of this step, in the case of a message, the MTA may generate a delivery report.

The MS or UA involved is called the delivery agent. A delivery agent is made known to the MTS by a process of registration, as a result of which the delivery agent and MTS keep one another informed of their names, their locations, and any other characteristics required for their interaction.

9.3.7 Retrieval

In a retrieval step, a user's MS conveys a message or report to its UA. The user in question is an actual recipient of the message or the originator of the subject message or probe. This step non-destructively retrieves the information object from storage. This step follows delivery or (a prior) retrieval.

This step may be taken only if the user is equipped with an MS.

9.3.8 Receipt

In a receipt step, either a UA conveys a message or report to its direct user, or the communication system that serves an indirect user conveys such an information object to that user. In either case, this step conveys the object to its ultimate destination.

In the case of a direct user, this step follows the object's delivery or first retrieval (only). In the case of an indirect user, it follows the information object's conveyance by the communication system serving the user. In either case, the user is a potential recipient (and, in the case of a direct user, an actual recipient) of the message in question, or the originator of the subject message or probe.

9.4 Transmittal Events

The kinds of events that may occur in a transmittal are listed in the first column of Table 6. For each listed kind, the second column indicates the kinds of information objects – messages, probes, and reports – for which such events may be staged, the third column the kinds of functional objects – users, UAs, MSs, MTAs, and AUs – that may stage such events.

All the events occur within the MTS.

Table 6 – Transmittal Events

Transmittal Event	Information Objects			Functional Objects				
	M	P	R	user	UA	MS	MTA	AU
splitting	x	x	-	-	-	-	x	-
joining	x	x	x	-	-	-	x	-
name resolution	x	x	-	-	-	-	x	-
DL expansion	x	-	-	-	-	-	x	-
redirection	x	x	-	-	-	-	x	-
conversion	x	x	-	-	-	-	x	-
non-delivery	x	-	x	-	-	-	x	-
non-affirmation	-	x	-	-	-	-	x	-
affirmation	-	x	-	-	-	-	x	-
routing	x	x	x	-	-	-	x	-

+ - Legend - - - - - +

M	message	x	permitted
P	probe		
R	report		

+ - - - - - +

The kinds of transmittal events, summarized in the table, are individually defined and described in the subclauses below.

9.4.1 Splitting

In a splitting event, an MTA replicates a message or probe, dividing responsibility for its immediate recipients among the resulting information objects. This event effectively allows an MTA to independently convey an object to various potential recipients.

An MTA stages a splitting when the next step or event required in the conveyance of a message or probe to some immediate recipients differs from that required in its conveyance to others.

9.4.2 Joining

In a joining event, an MTA combines several instances of the same message or probe, or two or more delivery and/or non-delivery reports for the same subject message or probe.

An MTA may, but need not stage a joining when it determines that the same events and next step are required to convey several highly related information objects to their destinations.

9.4.3 Name Resolution

In a name resolution event, an MTA adds the corresponding *OR-address* to the *OR-name* that identifies one of a message's or probe's immediate recipients.

9.4.4 DL Expansion

In a DL expansion event, an MTA replaces an immediate recipient which denotes a DL by the members of that DL, which are thereby made member recipients. DL expansion events occur only for messages, not for probes.

A particular DL is always subjected to DL expansion at a pre-established location within the MTS. This location is called the DL's expansion point and is identified by an *OR-address*.

As part of this event, the MTA may generate a delivery report.

DL expansion is subject to submit permission. In the case of a nested DL, that permission must have been granted to the DL of which the nested DL is a member. Otherwise, it must have been granted to the originator.

9.4.5 Redirection

In a redirection event, an MTA replaces a user or DL among a message's or probe's immediate recipients with an originator-specified or recipient-assigned alternate recipient.

9.4.6 Conversion

In a conversion event, an MTA transforms parts of a message's content from one EIT to another, or alters a probe so it appears that the described messages were so modified. This event increases the likelihood that an information object can be delivered or affirmed by tailoring it to its immediate recipients.

The following kinds of conversion are distinguished, on the basis of how the EIT of the information to be converted and the EIT to result from the conversion are selected:

- a) explicit conversion: A conversion in which the originator selects both the initial and final EITs.
- b) implicit conversion: A conversion in which the MTA selects the final EITs based upon the initial EITs and the capabilities of the UA.

9.4.7 Non-delivery

In a non-delivery event, an MTA determines that the MTS cannot deliver a message to its immediate recipients, or cannot deliver a report to the originator of its subject message or probe. This event halts the conveyance of an object the MTS deems unconveyable.

As part of this event, in the case of a message, the MTA generates a non-delivery report.

An MTA stages a non-delivery, e.g., when it determines that the immediate recipients are improperly specified, that they do not accept delivery of messages like that at hand, or that the message has not been delivered to them within pre-specified time limits.

9.4.8 Non-affirmation

In a non-affirmation event, an MTA determines that the MTS could not deliver a described message to a probe's immediate recipients. This event partially or fully determines the answer to the question posed by a probe.

As part of this event, the MTA generates a non-delivery report.

An MTA stages a non-affirmation, e.g., when it determines that the immediate recipients are improperly specified or would not accept delivery of a described message.

9.4.9 Affirmation

In an affirmation event, an MTA determines that the MTS could deliver any described message to a probe's immediate recipients. This event partially or fully determines the answer to the question posed by a probe, and elevates the immediate recipients to the status of actual recipients.

As part of this event, the MTA may generate a delivery report.

An MTA stages an affirmation once it determines that the immediate recipients are properly specified and, if the immediate recipients are users (but not DLs), would accept delivery of any described message. If the immediate recipients are DLs, an MTA stages an affirmation if the DL exists and the originator has the relevant submit permission.

9.4.10 Routing

In a routing event, an MTA selects the "adjacent" MTA to which it will transfer a message, probe, or report. This event incrementally determines an information object's route through the MTS and (obviously) may be taken only if the MTS comprises several MTAs.

The following kinds of routing are distinguished, on the basis of the kind of transfer for which they prepare:

- a) internal routing: A routing preparatory to an internal transfer (i.e., a transfer within an *MD*).
- b) external routing: A routing preparatory to an external transfer (i.e., a transfer between *MDs*).

An MTA stages a routing when it determines that it can stage no other event, and take no step, regarding an object.

10 Security Model

This clause provides an abstract security model for Message Transfer. The concrete realization of the model is the subject of other MHS Specifications. The security model provides a framework for describing the security services that counter potential threats (see annex D) to the MTS and the security elements that support those services.

The security features are an optional extension to the MHS that can be used to minimise the risk of exposure of assets and resources to violations of a security policy (threats). Their aim is to provide features independently of the communications services provided by other lower or higher entities. Threats may be countered by the use of physical security, computer security (COMPUSEC), or security services provided by the MHS. Depending on the perceived threats, certain of the MHS security services will be selected in combination with appropriate physical security and COMPUSEC measures. The security services supported by the MHS are described below. The naming and structuring of the services are based on ISO 7498-2.

NOTE – Despite these security features, certain attacks may be mounted against communication between a user and the MHS or against user-to-user communication (e.g., in the case of users accessing the MHS through an access unit, or in the case of users remotely accessing their UAs). To counter these attacks requires extensions to the present security model and services which are for future standardisation.

In many cases, the broad classes of threats are covered by several of the services listed.

The security services are supported through use of service elements of the Message Transfer Service message envelope. The envelope contains security relevant arguments as described in ITU-T Rec. X.411 | ISO/IEC 10021-4. The description of the security services takes the following general form. In 10.2 the services are listed, with, in each case, a definition of the service and an indication of how it may be provided using the security elements in ITU-T Rec. X.411 | ISO/IEC 10021-4. In 10.3 the security elements are individually described, with, in each case, a definition of the service element and references to its constituent arguments in ITU-T Rec. X.411 | ISO/IEC 10021-4.

Many of the techniques employed rely on encryption mechanisms. The security services in the MHS allow for flexibility in the choice of algorithms. However, in some cases only the use of asymmetric encryption has been fully defined in this Specification. A future version or addenda to this Specification may allow use of alternative mechanisms based on symmetric encipherment.

NOTE – The use of the terms "security service" and "security element" in this clause are not to be confused with the terms "service" and "element of service" as used in ITU-T Rec. X.400 | ISO/IEC 10021-1. The former terms are used in the present clause to maintain consistency with ISO 7498-2.

10.1 Security Policies

Security services in the MHS must be capable of supporting a wide range of security policies which extend beyond the confines of the MHS itself. The services selected and the threats addressed will depend on the individual application and levels of trust in parts of the system.

A security policy defines how the risk to and exposure of assets can be reduced to an acceptable level.

In addition, operation between different domains, each with their own security policy, will be required. As each domain will be subject to its own overall security policy, covering more than just the MHS, a bilateral agreement on interworking between two domains will be required. This must be defined so as not to conflict with the security policies for either domain and effectively becomes part of the overall security policy for each domain.

10.2 Security Services

This clause defines the Message Transfer security services. The naming and structuring of the services are based on ISO 7498-2.

Message Transfer security services fall into several broad classes. These classes and the services in each are listed in Table 7. An asterisk (*) under the heading of the form *X/Y* indicates that the service can be provided from a functional object of type *X* to one of type *Y*.

Table 7 – Message Transfer Security Services

SERVICE	UA/UA	MS/MTA	MTA/MS	MTA/UA	MS/UA
	UA/MS	UA/MTA	MTA/MTA	MTA/UA	
ORIGIN AUTHENTICATION					
Message Origin Authentication	*	*	-	*	-
Probe Origin Authentication	-	-	*	*	-
Report Origin Authentication	-	-	-	*	*
Proof of Submission	-	-	-	-	*
Proof of Delivery	*	-	-	-	-
SECURE ACCESS MANAGEMENT					
Peer Entity Authentication	-	*	*	*	*
Security Context	-	*	*	*	*
DATA CONFIDENTIALITY					
Connection Confidentiality	-	*	*	*	*
Content Confidentiality	*	-	-	-	-
Message Flow Confidentiality	*	-	-	-	-
DATA INTEGRITY SERVICES					
Connection Integrity	-	*	*	*	*
Content Integrity	*	-	-	-	-
Message Sequence Integrity	*	-	-	-	-
NON-REPUDIATION					
Non-repudiation of Origin	*	-	-	*	-
Non-repudiation of Submission	-	-	-	-	*
Non-repudiation of Delivery	*	-	-	-	-
MESSAGE SECURITY LABELLING					
Message Security Labelling	*	*	*	*	*
SECURITY MANAGEMENT SERVICES					
Change Credentials	-	*	-	*	*
Register	-	*	-	*	-
MS-Register	-	*	-	-	-

Note – This service is provided by the recipient's MS to the originator's UA.

Throughout the security service definitions that follow, reference is made to Figure 6, which reiterates the MHS functional model in simplified form. The numeric labels are referenced in the text.

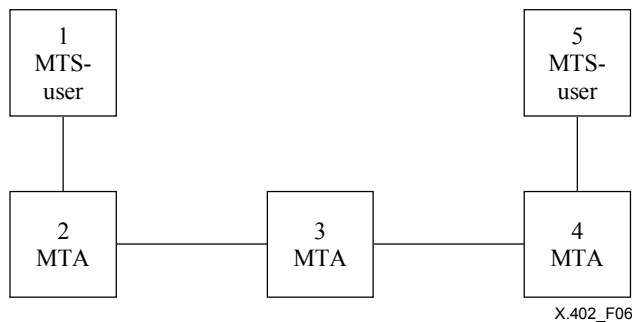


Figure 6 – Simplified MHS Functional Model

10.2.1 Origin Authentication Security Services

These security services provide for the authentication of the identity of communicating peer entities and sources of data.

10.2.1.1 Data Origin Authentication Security Services

These security services provide corroboration of the origin of a message, probe, or report to all concerned entities (i.e., MTAs or recipient MTS-users). These security services cannot protect against duplication of messages, probes, or reports.

10.2.1.1.1 Message Origin Authentication Security Service

The Message Origin Authentication Service enables the corroboration of the source of a message.

This security service can be provided using either the Message Origin Authentication or the Message Argument Integrity security element. The former can be used to provide the security service to any of the parties concerned (1-5 inclusive in Figure 6), whereas the latter can only be used to provide the security service to MTS-users (1 or 5 in Figure 6). The security element chosen depends on the prevailing security policy.

10.2.1.1.2 Probe Origin Authentication Security Service

The Probe Origin Authentication security service enables the corroboration of the source of a probe.

This security service can be provided by using the Probe Origin Authentication security element. This security element can be used to provide the security service to any of the MTAs through which the probe is transferred (2-4 inclusive in Figure 6).

10.2.1.1.3 Report Origin Authentication Security Service

The Report Origin Authentication security service enables the corroboration of the source of a report.

This security service can be provided by using the Report Origin Authentication security element. This security element can be used to provide the security service to the originator of the subject message or probe, as well as to any MTA through which the report is transferred (1-5 inclusive in Figure 6).

10.2.1.2 Proof of Submission Security Service

This security service enables the originator of a message to obtain corroboration that it has been received by the MTS for delivery to the originally specified recipient(s).

This security service can be provided by using the Proof of Submission security element.

10.2.1.3 Proof of Delivery Security Service

This security service enables the originator of a message to obtain corroboration that it has been delivered by the MTS to its intended recipient(s).

This security service can be provided by using the Proof of Delivery security element.

10.2.2 Secure Access Management Security Service

The Secure Access Management security service is concerned with providing protection for resources against their unauthorised use. It can be divided into two components, namely the Peer Entity Authentication and the Security Context security services.

10.2.2.1 Peer Entity Authentication Security Service

This security service is provided for use at the establishment of a connection to confirm the identity of the connecting entity. It may be used on the links 1-2, 2-3, 3-4, or 4-5 in Figure 6 and provides confidence, at the time of usage only, that an entity is not attempting a masquerade or an unauthorised replay of a previous connection.

This security service is supported by the Authentication Exchange security element. Note that use of this security element may yield other data as a result of its operation that in certain circumstances can be used to support a Connection Confidentiality and/or a Connection Integrity security service.

10.2.2.2 Security Context Security Service

This security service is used to limit the scope of passage of messages between entities by reference to the Security Labels associated with messages. This security service is therefore closely related to the Message Security Labelling security service, which provides for the association of messages and Security Labels.

The Security Context security service is supported by the Security Context and the Register security elements.

10.2.3 Data Confidentiality Security Services

These security services provide for the protection of data against unauthorised disclosure.

10.2.3.1 Connection Confidentiality Security Service

The MHS does not provide a Connection Confidentiality security service. However, data for the invocation of such a security service in underlying layers may be provided as a result of using the Authentication Exchange security element

to provide the Peer Entity Authentication security service. The security service may be required on any of links 1-2, 2-3, 3-4, or 4-5 in Figure 6.

10.2.3.2 Content Confidentiality Security Service

The Content Confidentiality security service provides assurance that the content of a message is only known to the sender and recipient of a message.

It may be provided using a combination of the Content Confidentiality and the Message Argument Confidentiality security elements. The Message Argument Confidentiality security element can be used to transfer a secret key which is used with the Content Confidentiality security element to encipher the message content. Using these security elements the service is provided from MTS-user 1 to MTS-user 5 in Figure 6, with the message content being unintelligible to MTAs.

10.2.3.3 Message Flow Confidentiality Security Service

This security service provides for the protection of information which might be derived from observation of message flow. Only a limited form of this security service is provided by the MHS.

The Double Enveloping Technique enables a complete message to become the content of another message. This could be used to hide addressing information from certain parts of the MTS. Used in conjunction with traffic padding (which is beyond the current scope of this Specification) this could be used to provide message flow confidentiality. Other elements of this service, such as routing control or pseudonyms, are also beyond the scope of this Specification.

10.2.4 Data Integrity Security Services

These security services are provided to counter active threats to the MHS.

10.2.4.1 Connection Integrity Security Service

The MHS does not provide a Connection Integrity security service. However, data for the invocation of such a security service in underlying layers may be provided by using the Authentication Exchange security element to provide the Peer Entity Authentication security service. The security service may be required on any of links 1-2, 2-3, 3-4, or 4-5 in Figure 6.

10.2.4.2 Content Integrity Security Service

This security service provides for the integrity of the contents of a single message. This takes the form of enabling the determination of whether the message content has been modified. This security service does not enable the detection of message replay, which is provided by the Message Sequence Integrity security service.

This security service can be provided in two different ways using two different combinations of security elements.

The Content Integrity security element together with the Message Argument Integrity security element and, in some cases, the Message Argument Confidentiality security element can be used to provide the security service to a message recipient, i.e., for communication from MTS-user 1 to MTS-user 5 in Figure 6. The Content Integrity security element is used to compute a Content Integrity Check as a function of the entire message content. Depending on the method used to compute the Content Integrity Check, a secret key may be required, which may be confidentially sent to the message recipient using the Message Argument Confidentiality security element. The Content Integrity Check is protected against change using the Message Argument Integrity security element. The integrity of any confidential message arguments is provided using the Message Argument Confidentiality security element.

The Message Origin Authentication security element can also be used to provide this security service.

10.2.4.3 Message Sequence Integrity Security Service

This security service protects the originator and recipient of a sequence of messages against re-ordering of the sequence. In doing so it protects against replay of messages.

This security service may be provided using a combination of the Message Sequence Integrity and the Message Argument Integrity security elements. The former provides a sequence number to each message, which may be protected against change by use of the latter. Simultaneous confidentiality and integrity of the Message Sequence Number may be provided by use of the Message Argument Confidentiality security element.

These security elements provide the service for communication from MTS-user 1 to MTS-user 5 in Figure 6, and not to the intermediate MTAs.

10.2.5 Non-Repudiation Security Services

These security services provide irrevocable proof to a third party after the message has been submitted, sent, or delivered, that the submission, sending, or receipt did occur as claimed. Note that for this to function correctly, the security policy must explicitly cover the management of asymmetric keys for the purpose of non-repudiation services if asymmetric algorithms are being used.

10.2.5.1 Non-repudiation of Origin Security Service

This security service provides the recipient(s) of a message with irrevocable proof of the origin of the message, its content, and its associated Message Security Label.

This security service can be provided in two different ways using two different combinations of security elements. Note that its provision is very similar to the provision of the (weaker) Content Integrity security service.

The Content Integrity security element together with the Message Argument Integrity security element and, in some cases, the Message Argument Confidentiality security element can be used to provide the service to a message recipient, i.e., for communication from MTS-user 1 to MTS-user 5 in Figure 6. The Content Integrity security element is used to compute a Content Integrity Check as a function of the entire message content. Depending on the method used to compute the Content Integrity Check, a secret key may be required, which may be confidentially sent to the message recipient using the Message Argument Confidentiality security element. The Content Integrity Check and, if required, the Message Security Label are protected against change and/or repudiation using the Message Argument Integrity security element. Any confidential message arguments are protected against change and/or repudiation using the Message Argument Confidentiality security element.

If the Content Confidentiality security service is not required, the Message Origin Authentication security element may also be used as a basis for this security service. In this case the security service may be provided to all elements of the MHS, i.e., for all of 1-5 in Figure 6.

10.2.5.2 Non-Repudiation of Submission Security Service

This security service provides the originator of the message with irrevocable proof that the message was submitted to the MTS for delivery to the originally specified recipient(s).

This security service is provided using the Proof of Submission security element in much the same way as that security element is used to support the (weaker) Proof of Submission security service.

10.2.5.3 Non-Repudiation of Delivery Security Service

This security service provides the originator of the message with irrevocable proof that the message was delivered to its originally specified recipient(s).

This security service is provided using the Proof of Delivery security element in much the same way as that security element is used to support the (weaker) Proof of Delivery security service.

10.2.6 Message Security Labelling Security Service

This security service allows Security Labels to be associated with all entities in the MHS, i.e., MTAs and MTS-users. In conjunction with the Security Context security service it enables the implementation of security policies defining which parts of the MHS may handle messages with specified associated Security Labels.

This security service is provided by the Message Security Label security element. The integrity and confidentiality of the label are provided by the Message Argument Integrity and the Message Argument Confidentiality security elements.

10.2.7 Security Management Services

A number of security management services are needed by the MHS. The only management services provided within ITU-T Rec. X.411 | ISO/IEC 10021-4 are concerned with changing credentials and registering MTS-user security labels.

10.2.7.1 Change Credentials Security Service

This security service enables one entity in the MHS to change the credentials concerning it held by another entity in the MHS. It may be provided using the Change Credentials security element.

10.2.7.2 Register Security Service

This security service enables the establishment at an MTA of the Security Labels which are permissible for one particular MTS-user. It may be provided using the Register security element.