INTERNATIONAL STANDARD

ISO/IEC 10021-2

Third edition
2003-12-15

Information technology — Message Handling Systems (MHS): Overall Architecture

Technologies de l'information — Systèmes de messagerie (MHS): Architecture globale

Reference number
ISO/IEC 10021-2:2003(E)

© ISO/IEC 2003

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

© ISO/IEC 2003

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

© ISO/IEC 2003 – All rights reserved

Not for Resale

CONTENTS

Page

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

© ISO/IEC 2003 All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Page

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

© ISO/IEC 2003 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Page

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

--`,,`-`-`,,`,,`,`,,`---
© ISO/IEC 2003 All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Page

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

© ISO/IEC 2003 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Page

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

© ISO/IEC 2003 All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 10021-2 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 6, *Telecommunications and information exchange between systems*, in collaboration with ITU-T. The identical text is published as ITU-T Rec. X.402.

This third edition cancels and replaces the second edition (ISO/IEC 10021-2:1996), which has been technically revised. It also incorporates Technical Corrigendum 1:1998.

ISO/IEC 10021 consists of the following parts, under the general title *Information technology — Message Handling Systems (MHS)*:

— *Part 1: System and Service Overview*

— *Part 2: Overall Architecture*

— *Part 4: Message transfer system: Abstract service definition and procedures*

— *Part 5: Message store: Abstract service definition*

— *Part 6: Protocol Specifications*

— *Part 7: Interpersonal messaging system*

— *Part 8: Electronic Data Interchange Messaging Service*

— *Part 9: Electronic Data Interchange Messaging System*

— *Part 10: MHS routing*

— *Part 11: MHS Routing — Guide for messaging systems managers* [Technical Report]

--`,,`-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

© ISO/IEC 2003 – All rights reserved

Not for Resale

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.

© ISO/IEC 2003 All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

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.*

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

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 10021-4:2003, *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 10021-6:2003, *Information technology – Message Handling Systems (MHS) – Protocol specifications.*
- ITU-T Recommendation X.420 (1999) | ISO/IEC 10021-7:2003, *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.*

--`,,`-`-`,,`,,`,`,,`---
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

– 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).

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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;

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

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.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

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.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

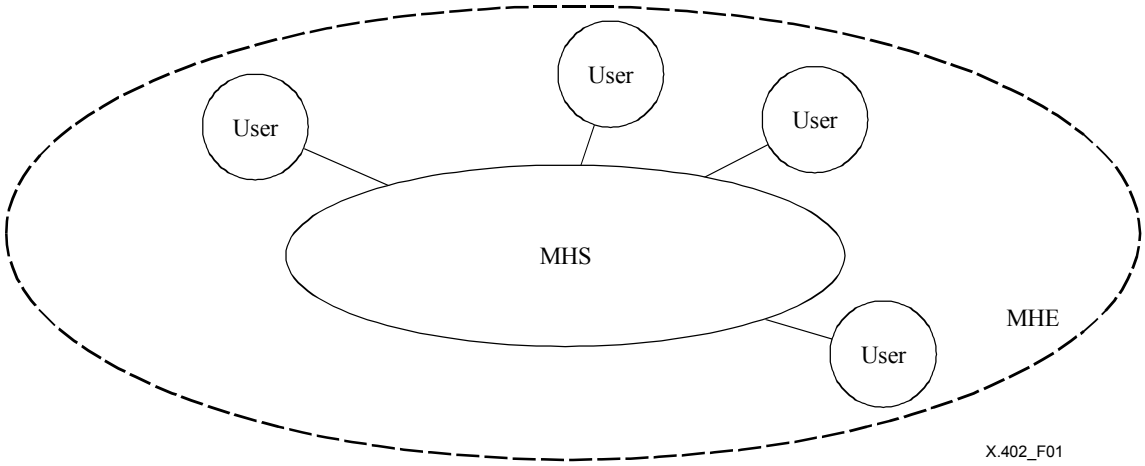


Figure 1 – The Message Handling Environment

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.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

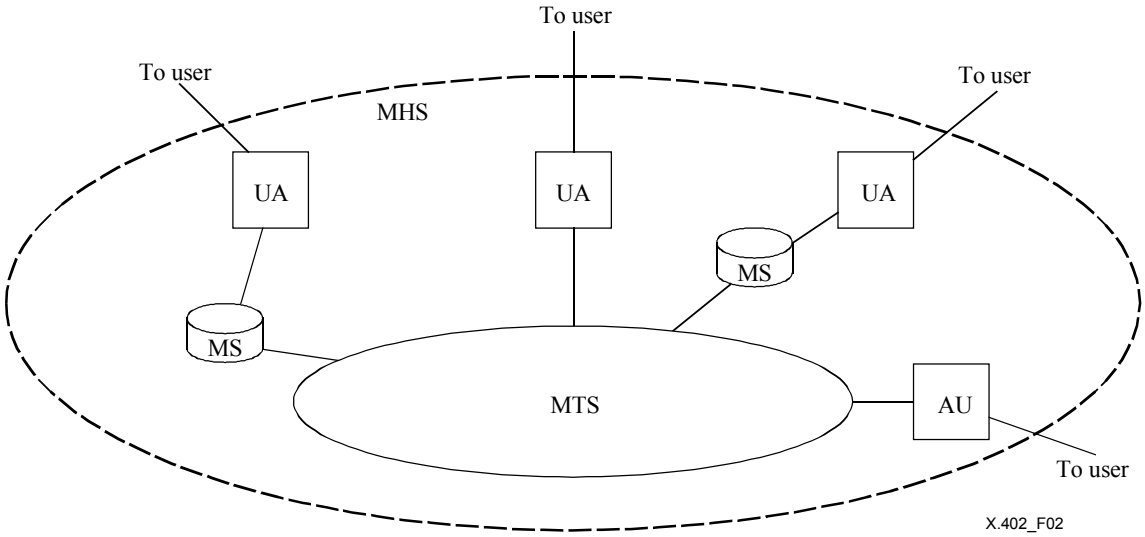


Figure 2 – The Message Handling System

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.

--`,,`-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

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.

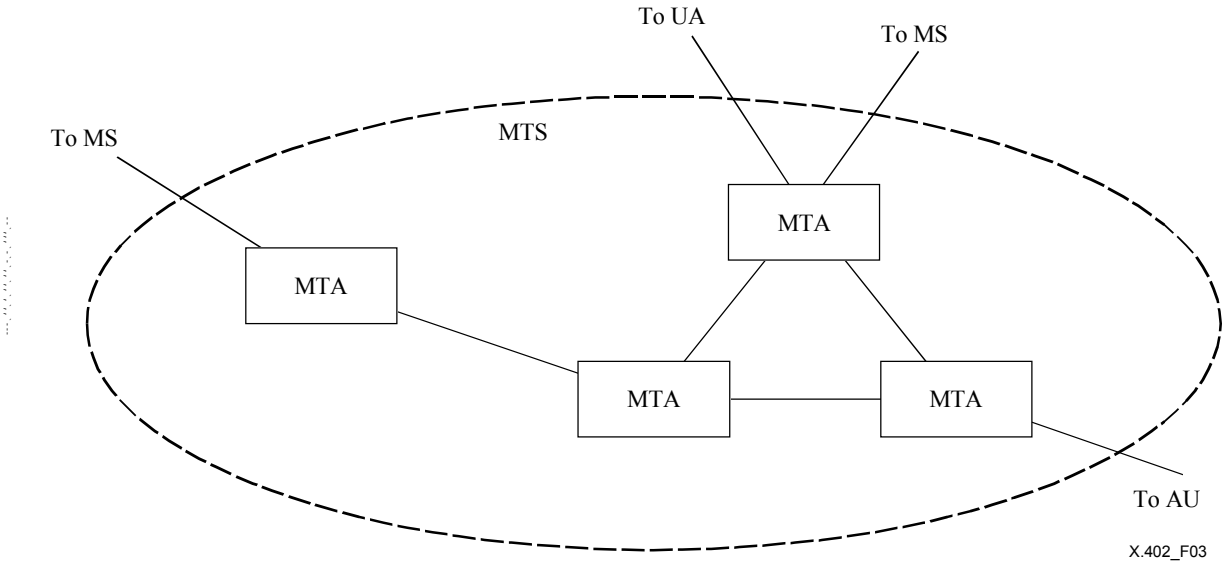


Figure 3 – The Message Transfer System

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 delevery*, 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 delevery 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 delevery*. 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.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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

Information 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.

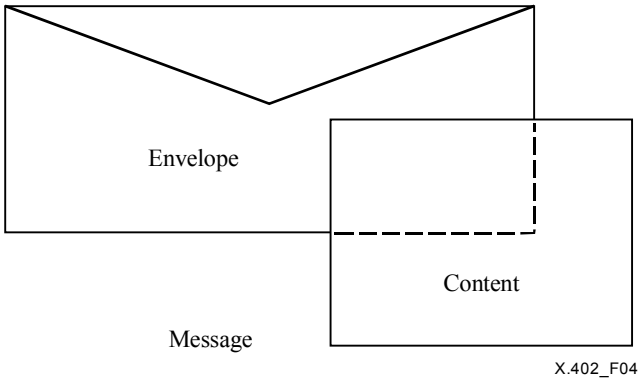


Figure 4 – A Message's Envelope and Content

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

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

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* comprisings *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 recipient*s, 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.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

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*.

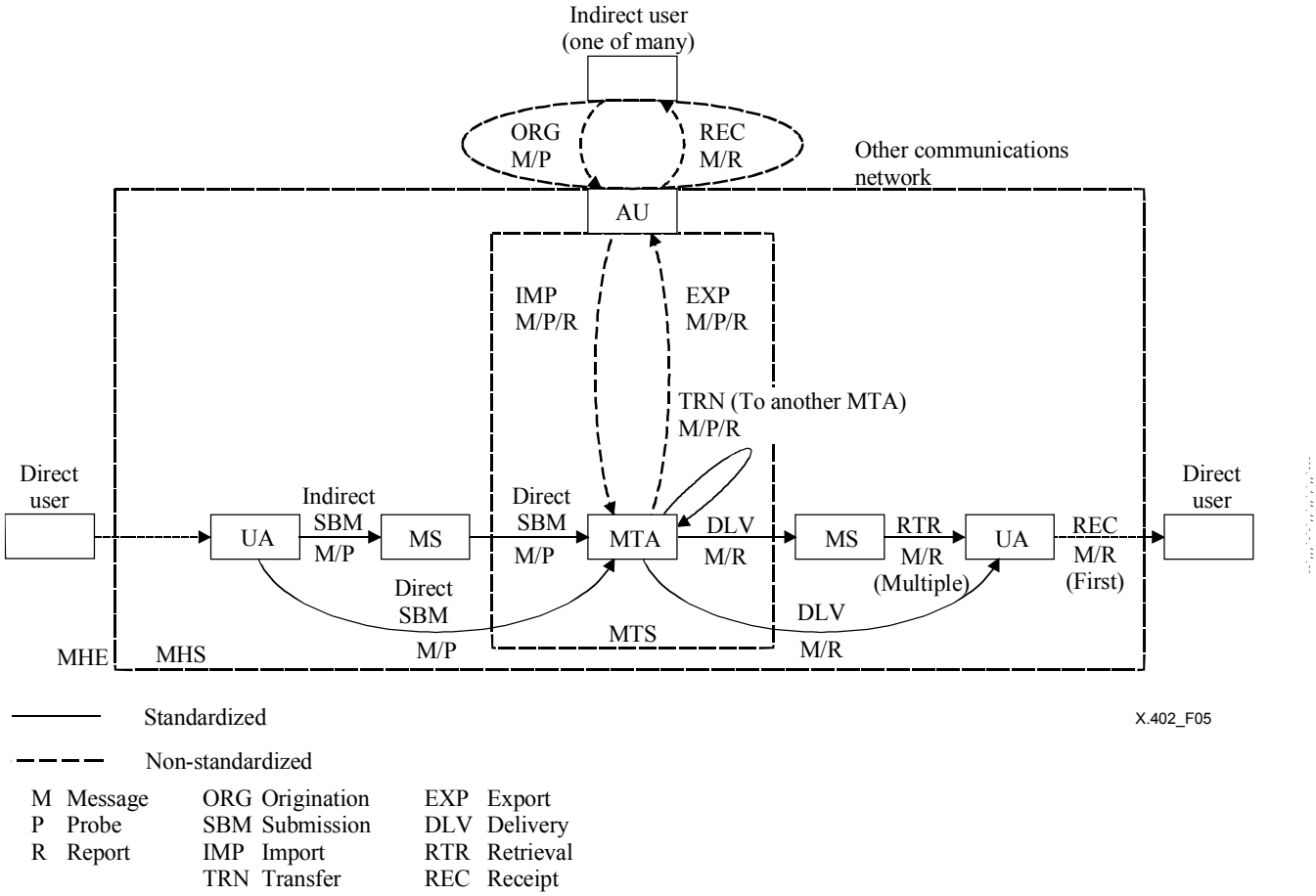


Figure 5 – The information flow of transmittal

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:

a) 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:

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

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.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

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

	Information Objects			Functional Objects				
Transmittal Event	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, P probe, R report; x permitted

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.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

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.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

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	UA/MS	UA/MTA	MTA/MTA	MTA/UA MS/UA
ORIGIN AUTHENTICATION								
Message Origin Authentication	*	*	–	*	–	–	–	–
Probe Origin Authentication	–	–	*	*	–	–	–	–
Report Origin Authentication	–	–	–	–	*	*	*	–
Proof of Submission	–	–	–	–	–	–	*	–
Proof of Delivery	*	–	–	–	–	–	–	Note
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	*	–	–	–	–	–	–	Note
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.

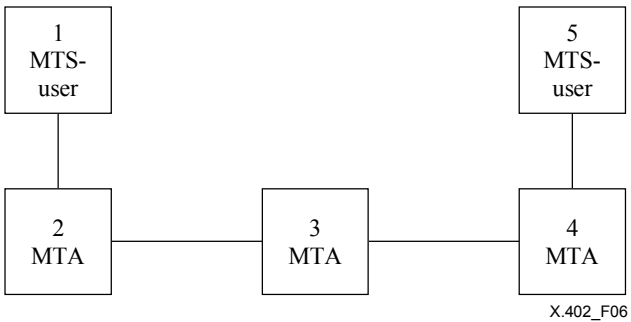


Figure 6 – Simplified MHS Functional Model

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.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

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

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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.

--`,,`--`,,`,,`,`,,`---
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

10.2.7.3 MS-Register Security Service

This security service enables the establishment of the security label which are permissible for the MS-user.

10.3 Security Elements

The following subclauses describe the security elements available in the protocols described within ITU-T Rec. X.411 | ISO/IEC 10021-4 to support the security services in the MHS. These security elements relate directly to arguments in various services described in ITU-T Rec. X.411 | ISO/IEC 10021-4. The objective of this clause is to separate out each element of the ITU-T Rec. X.411 | ISO/IEC 10021-4 service definitions that relate to security, and to define the function of each of these identified security elements.

10.3.1 Authentication Security Elements

These security elements are defined in order to support authentication and integrity security services.

10.3.1.1 Authentication Exchange Security Element

The Authentication Exchange security element is designed to authenticate, possibly mutually, the identity of an MTS user to an MTA, an MTA to an MTA, an MTA to an MTS-user, an MS to a UA, or a UA to an MS. It is based on the exchange or use of secret data, either passwords, asymmetrically encrypted tokens, or symmetrically encrypted tokens. The result of the exchange is corroboration of the identity of the other party, and, optionally, the transfer of confidential data which may be used in providing the Connection Confidentiality and/or the Connection Integrity security service in underlying layers. Such an authentication is only valid for the instant that it is made and the continuing validity of the authenticated identity depends on whether the exchange of confidential data, or some other mechanism, is used to establish a secure communication path. The establishment and use of a secure communication path is outside the scope of this Specification.

This security element uses the Initiator Credentials argument and the Responder Credentials result of the MTS-bind, MS-bind, and MTA-bind services. The transferred credentials are either passwords or tokens.

Where passwords are used for authentication, these may be either simple passwords or protected passwords. The use of protected passwords for authentication between UA and MS is described in detail in Annex H.

NOTE – Although Annex H describes authentication between UA and MS, apart from the protected mechanism to change the password it applies equally to authentication between UA and MTA.

10.3.1.2 Data Origin Authentication Security Elements

These security elements are specifically designed to support data origin authentication services, although they may also be used to support certain data integrity services.

10.3.1.2.1 Message Origin Authentication Security Element

The Message Origin Authentication security element enables anyone who receives or transfers message to authenticate the identity of the MTS-user that originated the message. This may mean the provision of the Message Origin Authentication or the Non-repudiation of Origin security service.

The security element involves transmitting, as part of the message, a Message Origin Authentication Check, computed as a function of the message content, the message Content Identifier, and the Message Security Label. If the Content Confidentiality security service is also required, the Message Origin Authentication Check is computed as a function of the enciphered rather than the unenciphered message content. By operating on the message content as conveyed in the overall message (i.e., after the optional Content Confidentiality security element), any MHS entity can check the overall message integrity without the need to see the plaintext message content. However, if the Content Confidentiality security service is used, the Message Origin Authentication security element cannot be used to provide the Non-repudiation of Origin security service.

The security element uses the Message Origin Authentication Check, which is one of the arguments of the Message Submission, Message Transfer, and Message Delivery services.

10.3.1.2.2 Probe Origin Authentication Security Element

Similar to the Message Origin Authentication security element, the Probe Origin Authentication security element enables any MTA to authenticate the identity of the MTS-user which originated a probe.

This security element uses the Probe Origin Authentication Check, which is one of the arguments of the Probe Submission service.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

10.3.1.2.3 Report Origin Authentication Security Element

Similar to the Message Origin Authentication security element, the Report Origin Authentication security element enables any MTA or MTS-user who receives a report to authenticate the identity of the MTA which originated the report.

This security element uses the Report Origin Authentication Check, which is one of the arguments of the Report Delivery service.

10.3.1.3 Proof of Submission Security Element

This security element provides the originator of a message with the means to establish that a message was accepted by the MHS for transmission.

The security element is made up of two arguments: a request for Proof of Submission, sent with a message at submission time, and the Proof of Submission, returned to the MTS-user as part of the Message Submission results. The Proof of Submission is generated by the MTS, and is computed as a function of all the arguments of the submitted message, the Message Submission Identifier, and the Message Submission Time.

The Proof of Submission argument can be used to support the Proof of Submission security service. Depending on the security policy in force, it may also be able to support the (stronger) Non-repudiation of Submission security service.

The Proof of Submission Request is an argument of the Message Submission service. The Proof of Submission is one of the results of the Message Submission service.

10.3.1.4 Proof of Delivery Security Element

This security element provides the originator of a message with the means to establish that a message was delivered to the destination by the MHS.

The security element is made up of a number of arguments. The message originator includes a Proof of Delivery Request with the submitted message, and this request is delivered to each recipient with the message. A recipient may then compute the Proof of Delivery as a function of a number of arguments associated with the message. The proof of delivery is returned by the MTS to the message originator, as part of a report on the results of the original Message Submission.

The Proof of Delivery can be used to support the Proof of Delivery security service. Depending on the security policy in force, it may also be able to support the (stronger) Non-repudiation of Delivery security service.

The Proof of Delivery Request is an argument of the Message Submission, Message Transfer, and Message Delivery services. The Proof of Delivery is both one of the results of the Message Delivery service and one of the arguments of the Report Transfer and Report Delivery services.

NOTE – Non-receipt of a Proof of Delivery does not imply non-delivery.

10.3.2 Secure Access Management Security Elements

These security elements are defined in order to support the Secure Access Management security service and the security management services.

10.3.2.1 Security Context Security Element

When an MTS-user or an MTA binds to an MTA or MTS-user, the bind operation specifies the security context of the connection. This limits the scope of passage of messages by reference to the labels associated with messages. Secondly, the Security Context of the connection may be temporarily altered for submitted or delivered messages.

The Security Context itself consists of one or more Security Labels defining the sensitivity of interactions that may occur in line with the security policy in force.

Security Context is an argument of the MTS-bind and MTA-bind services.

10.3.2.2 Register Security Element

The Register security element allows the establishment at an MTA of an MTS-user's permissible security labels.

This security element is provided by the Register service. The Register service enables an MTS-user to change arguments, held by the MTS, relating to delivery of messages to that MTS-user.

10.3.2.3 MS-Register Security Element

The MS-Register security element allows the establishment of the MS-user's permissible security labels.

--`,,`-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

This security element is provided by the MS-Register service. The MS-Register service enables an MS-user to change arguments held by the MS relating to the retrieval of messages to that MS-user.

10.3.3 Data Confidentiality Security Elements

These security elements, based on the use of encipherment, are all concerned with the provision of confidentiality of data passed from one MHS entity to another.

10.3.3.1 Content Confidentiality Security Element

The Content Confidentiality security element provides assurance that the content of the message is protected from eavesdropping during transmission by use of an encipherment security element. The security element operates such that only the recipient and sender of the message know the plaintext message content.

The specification of the encipherment algorithm, the key used, and any other initialising data are conveyed using the Message Argument Confidentiality and the Message Argument Integrity security elements. The algorithm and key are then used to encipher or decipher the message contents.

The Content Confidentiality security element uses the Content Confidentiality Algorithm Identifier, which is an argument of the Message Submission, Message Transfer, and Message Delivery services.

10.3.3.2 Message Argument Confidentiality Security Element

The Message Argument Confidentiality security element provides for the confidentiality, integrity, and, if required, the irrevocability of recipient data associated with a message. Specifically, this data will comprise any cryptographic keys and related data that is necessary for the confidentiality and integrity security elements to function properly, if these optional security elements are invoked.

The security element operates by means of the Message Token. The data to be protected by the Message Argument Confidentiality security element constitutes the Encrypted Data within the Message Token. The Encrypted Data within the Message Token is unintelligible to all MTAs.

The Message Token is an argument of the Message Submission, Message Transfer, and Message Delivery services.

10.3.4 Data Integrity Security Elements

These security elements are provided to support the provision of data integrity, data authentication, and non-repudiation services.

10.3.4.1 Content Integrity Security Element

The Content Integrity security element provides protection for the content of a message against modification during transmission.

This security element operates by use of one or more cryptographic algorithms. The specification of the algorithm(s), the key(s) used, and any other initialising data are conveyed using the Message Argument Confidentiality and the Message Argument Integrity security elements. The result of the application of the algorithms and key is the Content Integrity Check, which is sent in the message envelope. The security element is only available to the recipient(s) of the message as it operates on the plaintext message contents.

If the Content Integrity Check is protected using the Message Argument Integrity security element then, depending on the prevailing security policy, it may be used to help provide the Non-repudiation of Origin security service.

The Content Integrity Check is an argument of the Message Submission, Message Transfer, and Message Delivery services.

10.3.4.2 Message Argument Integrity Security Element

The Message Argument Integrity security element provides for the integrity, and, if required, the irrevocability of certain arguments associated with a message. Specifically, these arguments may comprise any selection of the Content Confidentiality Algorithm Identifier, the Content Integrity Check, the Message Security Label, the Proof of Delivery Request, and the Message Sequence Number.

The security element operates by means of the Message Token. The data to be protected by the Message Argument Integrity security element constitutes the signed-data within the Message Token.

The Message Token is an argument of the Message Submission, Message Transfer, and Message Delivery services.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

10.3.4.3 Message Sequence Integrity Security Element

The Message Sequence Integrity security element provides protection for the sender and recipient of a message against receipt of messages in the wrong order, or duplicated messages.

A Message Sequence Number is associated with an individual message. This number identifies the position of a message in a sequence from one originator to one recipient. Therefore each originator-recipient pair requiring to use this security element will have to maintain a distinct sequence of message numbers. This security element does not provide for initialisation or synchronisation of Message Sequence Numbers.

10.3.5 Non-repudiation Security Elements

There are no specific Non-repudiation security elements defined in ITU-T Rec. X.411 | ISO/IEC 10021-4. The non-repudiation services may be provided using a combination of other security elements.

10.3.6 Security Label Security Elements

These security elements exist to support security labelling in the MHS.

10.3.6.1 Message Security Label Security Element

Messages may be labelled with data as specified in the prevailing security policy. The Message Security Label is available for use by intermediate MTAs as part of the overall security policy of the system.

A Message Security Label may be sent as a message argument, and may be protected by the Message Argument Integrity or the Message Origin Authentication security element, in the same manner as other message arguments.

Alternatively, if both confidentiality and integrity are required, the Message Security Label may be protected using the Message Argument Confidentiality security element. In this case the Message Security Label so protected is an originator-recipient argument, and may differ from the Message Security Label in the message envelope.

10.3.7 Security Management Security Elements

10.3.7.1 Change Credentials Security Element

The Change Credentials security element allows the credentials of an MTS-user or an MTA to be updated.

The security element is provided by the MTS Change Credentials service.

10.3.8 Double Enveloping Technique

Additional protection may be provided to a complete message, including the envelope parameters, by the ability to specify that the content of a message is itself a complete message, i.e., a Double Enveloping Technique is available.

This technique is available though the use of the Content Type argument which makes it possible to specify that the content of a message is an Inner Envelope. This Content Type means that the content is itself a message (envelope and content). When delivered to the recipient named on the outer envelope, the outer envelope is removed and the content is deciphered, if needed, resulting in an Inner Envelope and its content. The information contained in the Inner Envelope is used to transfer the content of the Inner Envelope to the recipients named on the Inner Envelope.

The Content Type is an argument of the Message Submission, Message Transfer, and Message Delivery services.

10.3.9 Encoding for Encryption and Hashing

Each MTS parameter being passed to encryption or hashing algorithms shall be encoded using ASN.1 encoding rules specified for the purpose of that encryption or hashing.

NOTE 1 – It cannot be assumed that the encoding of MTS parameters used in the Submission, Transfer or Delivery steps will use the encoding rules specified in the algorithm identifier.

NOTE 2 – In the case of the content, it is only the encoding of the content octets into the Octet String to which the encoding rules specified in the algorithm identifier should be applied, not the encoding of the content protocol (which remains unaltered).

SECTION 3 – CONFIGURATIONS

11 Overview

This section specifies how one can configure the MHS to satisfy any of a variety of functional, physical, and organizational requirements.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

This section covers the following topics:

a) Functional configurations;

b) Physical configurations;

c) Organizational configurations;

d) The *Global MHS*.

12 Functional Configurations

This clause specifies the possible functional configurations of the MHS. The variety of such configurations results from the presence or absence of the Directory, and from whether a direct user employs an MS.

12.1 Regarding the Directory

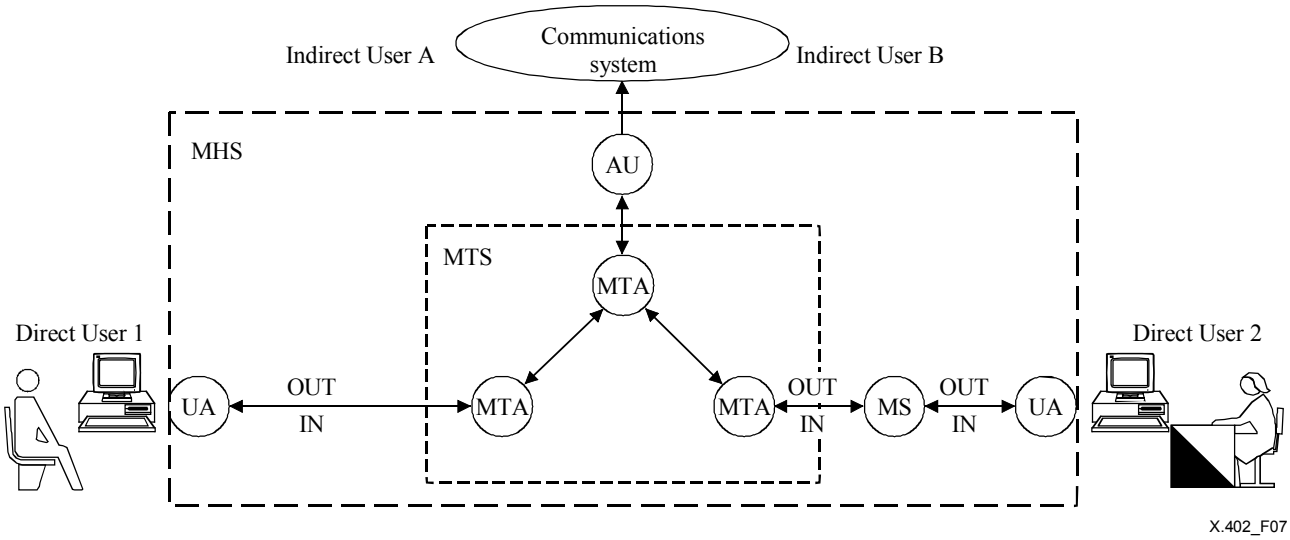
With respect to the Directory, the MHS can be configured for a particular user, or a collection of users (e.g., see 14.1), in either of two ways: with or without the Directory. A user without access to the Directory may lack the capabilities described in section five.

NOTE – A partially, rather than fully interconnected Directory may exist for an interim period during which the (global) Directory made possible by Recommendations | International Standards for Directories is under construction.

12.2 Regarding the Message Store

With respect to the MS, the MHS can be configured for a particular direct user in either of two ways: with or without an MS. A user without access to an MS lacks the capabilities of Message Storage. A user in such circumstances depends upon his UA for the storage of information objects, a capability that is a local matter.

The two functional configurations identified above are depicted in Figure 7 which also illustrates one possible configuration of the MTS, and its linkage to another communication system via an AU. In the figure, user 2 is equipped with an MS while user 1 is not.



NOTE – While the users depicted in this figure are people, this figure applies with equal force and validity to users of other kinds.

Figure 7 – Functional Configurations Regarding the MS

NOTE – While the users depicted in the figure are people, the figure applies with equal force and validity to users of other kinds.

13 Physical Configurations

This clause specifies the possible physical configurations of the MHS, i.e., how the MHS can be realized as a set of interconnected computer systems. Because the number of configurations is unbounded, the clause describes the kinds of *messaging systems* from which the MHS is assembled, and identifies a few important representative configurations.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

13.1 Messaging Systems

The building blocks used in the physical construction of the MHS are called *messaging systems*. A messaging system is a computer system (possibly but not necessarily an open system) that contains, or realizes, one or more functional objects.

Messaging systems are of the types depicted in Figure 8.

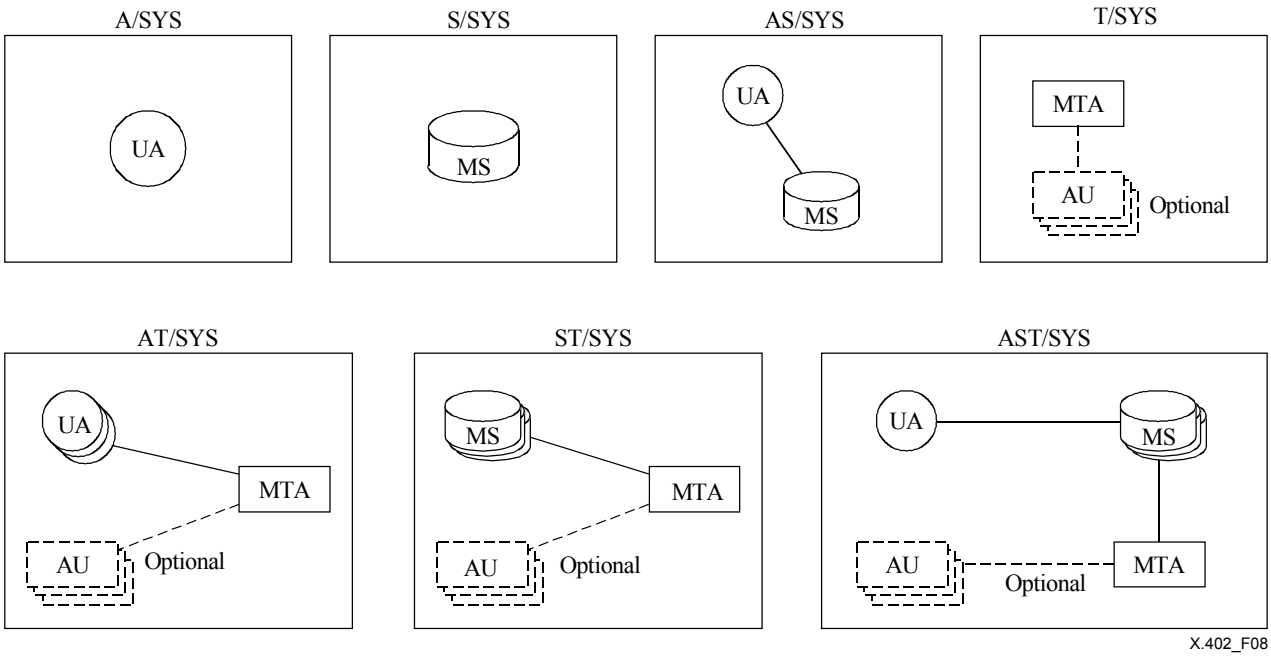


Figure 8 – Messaging System Types

The types of messaging system, depicted in the figure, are listed in the first column of Table 8. For each type listed, the second column indicates the kinds of functional object--UAs, MSs, MTAs, and AUs--that may be present in such a messaging system, whether their presence is mandatory or optional, and whether just one or possibly several of them may be present in the messaging system.

The table is divided into two sections. Messaging systems of the types in the first section are dedicated to single users, those of the types in the second can (but need not) serve multiple users.

Table 8 – Messaging Systems

Messaging System	Functional Objects			
	UA	MS	MTA	AU
A/SYS	1	–	–	–
S/SYS	–	1	–	–
AS/SYS	1	1	–	–
T/SYS	–	–	1	[M]
AT/SYS	M	–	1	[M]
ST/SYS	–	M	1	[M]
AST/SYS	M	M	1	[M]

+- Legend -------------------+
| M multiple [...] optional |
+----------------------------+

The messaging system types, summarized in the table, are individually defined and described in the subclauses below.

NOTE – The following major principles governed the admission of messaging system types:

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

a) An AU and the MTA with which it interacts are typically co-located because no protocol to govern their interaction is standardized.

b) An MTA is typically co-located with multiple UAs or MSs because, of the standardized protocols, only that for transfer simultaneously conveys a message to multiple recipients. The *serial* delivery of a message to multiple recipients served by a messaging system, which the delivery protocol would require, would be inefficient.

c) No purpose is served by co-locating several MTAs in a messaging system because a single MTA serves multiple users, and the purpose of an MTA is to convey objects between, not within such systems. (This is not intended to exclude the possibility of several MTA-related processes co-existing within a single computer system.)

d) The co-location of an AU with an MTA does not affect that system's behaviour with respect to the rest of the MHS. A single messaging system type, therefore, encompasses the AU's presence and absence.

13.1.1 Access Systems

An access system (A/SYS) contains one UA and neither an MS, an MTA, nor an AU.

An A/SYS is dedicated to a single user.

13.1.2 Storage Systems

A storage system (S/SYS) contains one MS and neither a UA, an MTA, nor an AU.

An S/SYS is dedicated to a single user.

13.1.3 Access and Storage Systems

An access and storage system (AS/SYS) contains one UA, one MS, and neither an MTA nor an AU.

An AS/SYS is dedicated to a single user.

13.1.4 Transfer Systems

A transfer system (T/SYS) contains one MTA; optionally, one or more AUs; and neither a UA nor an MS.

A T/SYS can serve multiple users.

13.1.5 Access and Transfer Systems

An access and transfer system (AT/SYS) contains one or more UAs; one MTA; optionally, one or more AUs; and no MS.

An AT/SYS can serve multiple users.

13.1.6 Storage and Transfer Systems

A storage and transfer system (ST/SYS) contains one or more MSs; one MTA; optionally, one or more AUs; and no UA.

An ST/SYS can serve multiple users.

13.1.7 Access, Storage, and Transfer Systems

An access, storage, and transfer system (AST/SYS) contains one or more UAs; one or more MSs; one MTA; and optionally, one or more AUs.

An AST/SYS can serve multiple users.

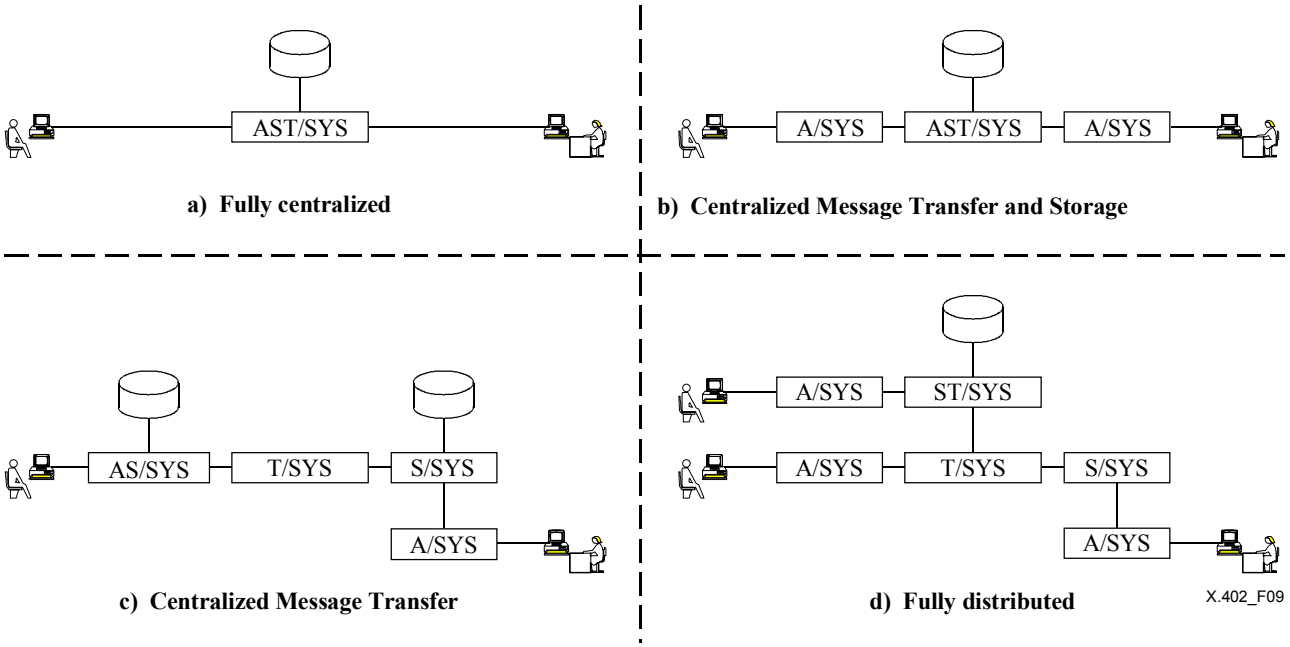
13.2 Representative Configurations

Messaging systems can be combined in various ways to form the MHS. The possible physical configurations are unbounded in number and thus cannot be enumerated. Several important representative configurations, however, are described below and in Figure 9.

13.2.1 Fully Centralized

The MHS may be fully centralized (panel *a* of the figure). This design is realized by a single AST/SYS which contains functional objects of all kinds and which can serve multiple users.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale



NOTES

1 While the users depicted in the figure are people, the figure applies with equal force and validity to users of other kinds.

2 Besides the physical configurations that result from the "pure" approaches below, many "hybrid" configurations can be constructed.

Figure 9 –Representative Physical Configurations

13.2.2 Centralized Message Transfer and Storage

The MHS may provide both Message Transfer and Message Storage centrally but distribute the user access (panel *b* of the figure). This design is realized by a single ST/SYS and, for each user, an A/SYS.

13.2.3 Centralized Message Transfer

The MHS may provide Message Transfer centrally but distribute the Message Storage and user access (panel *c* of the figure). This design is realized by a single T/SYS and, for each user, either an AS/SYS alone or an S/SYS and an associated A/SYS.

13.2.4 Fully Distributed

The MHS may distribute Message Transfer (panel *d* of the figure). This design involves multiple ST-SYSs or T-SYSs.

14 Organizational Configurations

This clause specifies the possible organizational configurations of the MHS, i.e., how the MHS can be realized as interconnected but independently managed sets of messaging systems (which are themselves interconnected). Because the number of configurations is unbounded, the clause describes the kinds of *management domains* from which the MHS is assembled, and identifies a few important representative configurations.

14.1 Management Domains

The primary building blocks used in the organizational construction of the MHS are called *management domains*. A management domain (MD) (or domain) is a set of messaging systems--at least one of which contains, or realizes, an MTA--that is managed by a single organization.

The above does not preclude an organization from managing a set of messaging systems (e.g., a single A/SYS) that does not qualify as an MD for lack of an MTA. Such a collection of messaging systems, a secondary building block used in the MHS' construction, "attaches" to an MD.

MDs are of several types which are individually defined and described in the subclauses below.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

14.1.1 Administration Management Domains

An administration management domain (ADMD) offers public message handling services to PRMDs and/or individual users. An ADMD has Administration responsibilities in order to ensure that its customers can communicate with any other MD attached to the *Global MHS*.

14.1.2 Private Management Domains

A private management domain (PRMD) comprises messaging systems managed by a private organization. While there is no restriction on a PRMD offering public messaging services, the PRMD has not accepted the Administration responsibilities in order to ensure its customers can communicate with any other MD attached to the *Global MHS*.

14.2 Representative Configurations

MDs can be combined in various ways to form the MHS. The possible organizational configurations are unbounded in number and thus cannot be enumerated. Several important representative configurations, however, are described below and in Figure 10.

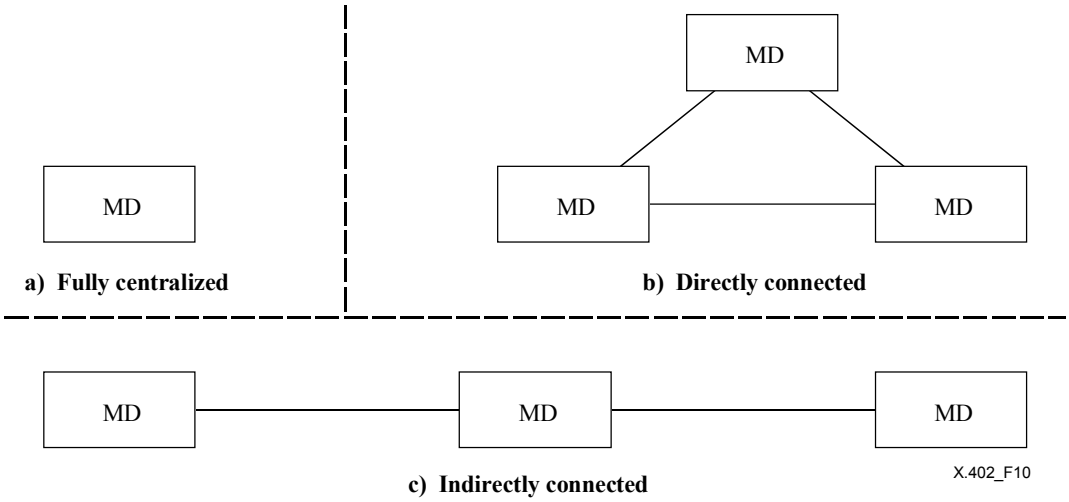


Figure 10 – Representative organizational configurations

NOTE – Besides the organizational configurations that result from the "pure" approaches below, many "hybrid" configurations can be constructed.

14.2.1 Fully Centralized

The entire MHS may be managed by one organization (panel *a* of the figure). This design is realized by a single MD.

14.2.2 Directly Connected

The MHS may be managed by several organizations, the messaging systems of each connected to the messaging systems of all of the others (panel *b* of the figure). This design is realized by multiple MDs interconnected pair-wise.

14.2.3 Indirectly Connected

The MHS may be managed by several organizations, the messaging systems of one serving as intermediary between the messaging systems of the others (panel c of the figure). This design is realized by multiple MDs one of which is interconnected to all of the others.

15 The Global MHS

A major purpose of MHS Specifications is to enable the construction of the Global MHS, an MHS providing both intra- and inter-organizational, and both intra- and international Message Handling world-wide.

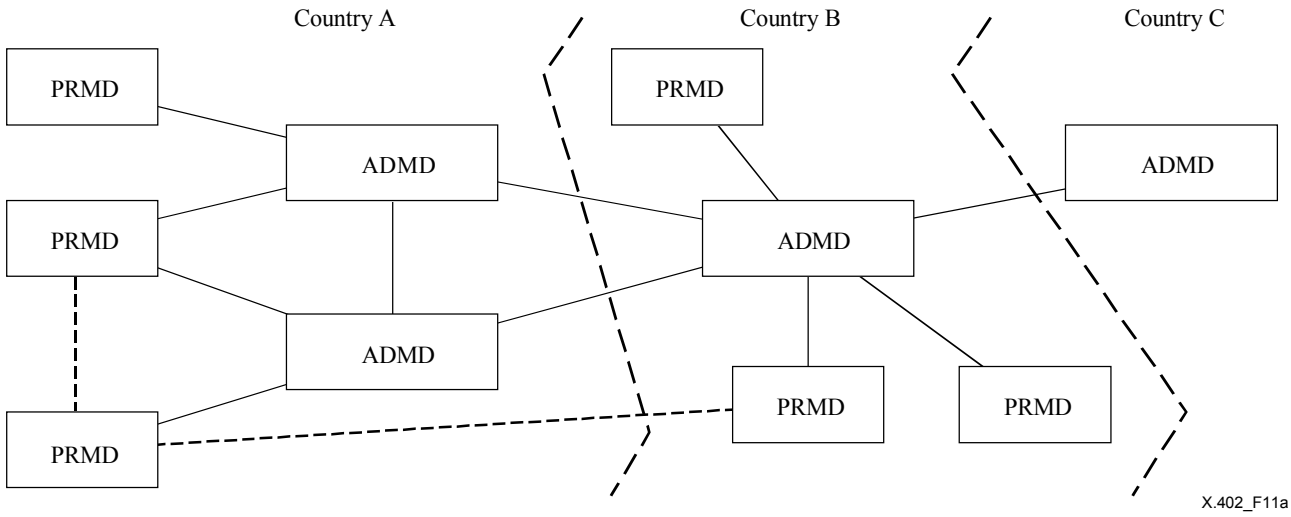
The Global MHS almost certainly encompasses the full variety of functional configurations specified in clause 12.

The physical configuration of the Global MHS is a hybrid of the pure configurations specified in clause 13, extremely complex and highly distributed physically.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

The organizational configuration of the Global MHS is a hybrid of the pure configurations specified in clause 14, extremely complex and highly distributed organisationally.

Figure 11 gives an example of possible interconnections. It does not attempt to identify all possible configurations. As depicted, ADMDs play a central role in the Global MHS. By interconnecting to one another internationally, they provide an international Message Transfer backbone. Depending upon national regulations, by interconnecting to one another domestically, they may also provide domestic backbones joined to the international backbone.



NOTE – The availability of the interconnections represented by the dotted lines between MTAs may be impacted by regulation.

Figure 11 – The global MHS

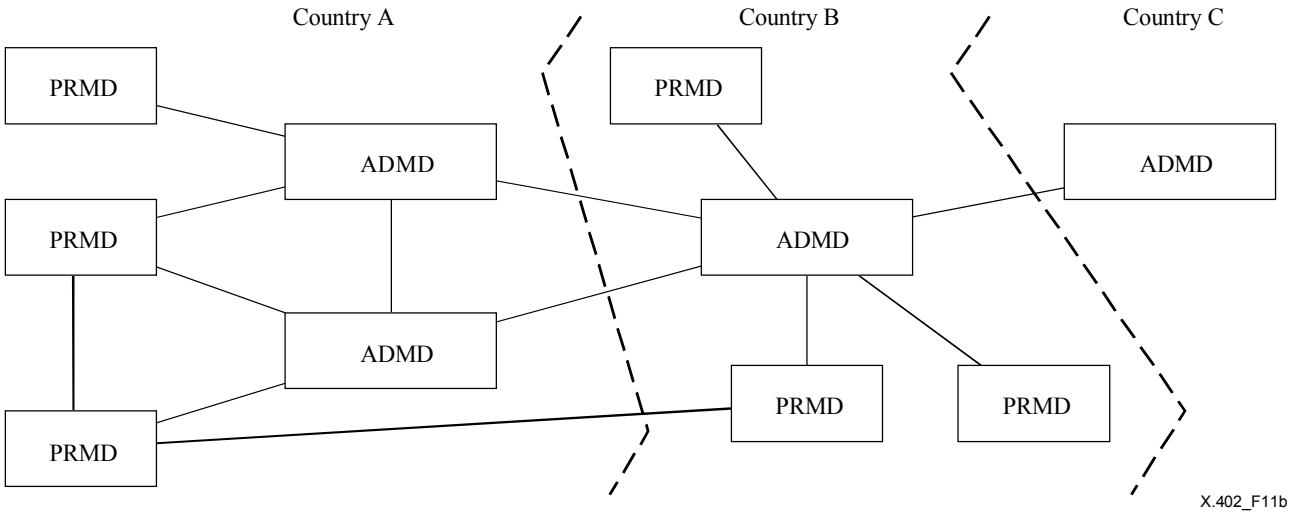


Figure 11 – The global MHS

SECTION 4 – NAMING, ADDRESSING, AND ROUTING

16 Overview

This section describes the naming and addressing of users and DLs and the routing of information objects to them.

This section covers the following topics:

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

a) Naming;

b) Addressing;

c) Routing.

17 Naming

This clause specifies how users and DLs are named for the purposes of Message Handling in general and Message Transfer in particular. It defines *OR-names* and describes the role that Directory names play in them.

When it directly submits a message or probe, a UA or MS identifies its potential recipients to the MTS. When the MTS delivers a message, it identifies the originator to each recipient's UA or MS. *OR-names* are the data structures by means of which such identification is achieved.

17.1 Directory Names

A Directory name is one component of an *OR-name*. A Directory name identifies an object to the Directory. By presenting such a name to the Directory, the MHS can access a user's or DL's Directory entry. From that entry the MTS can obtain, e.g., the user's or DL's *OR-address*.

Not every user or DL is registered in the Directory and, therefore, not every user or DL possesses a Directory name.

NOTE 1 – Many users and DLs will lack Directory names until the Directory is widely available as an adjunct to the MHS. Many indirect users (e.g., postal patrons) will lack such names until the Directory is widely available as an adjunct to other communication systems.

NOTE 2 – Users and DLs may be assigned Directory names even before a fully interconnected, distributed Directory has been put in place by pre-establishing the naming authorities upon which the Directory will eventually depend.

NOTE 3 – The typical Directory name is more user-friendly and more stable than the typical *OR-address* because the latter is necessarily couched in terms of the organizational or physical structure of the MHS while the former need not be. Therefore, it is intended that over time, Directory names become the primary means by which users and DLs are identified outside the MTS (i.e., by other users), and that the use of *OR-addresses* be largely confined to the MTS (i.e., to use by MTAs).

17.2 OR-Names

Every user or DL has one or more *OR-names*. An OR-name is an identifier by means of which a user can be designated as the originator, or a user or DL designated as a potential recipient of a message or probe. An OR-name distinguishes one user or DL from another and may also identify its point of access to the MHS.

An OR-name comprises a Directory name, an *OR-address*, or both. If present, the Directory name (if valid) unambiguously identifies the user or DL (but is not necessarily the only name that would do so). If present, the *OR-address* does the same and more (again see 18.5).

At direct submission, the UA or MS of the originator of a message or probe may include either or both components in each OR-name it supplies. If the *OR-address* is omitted, the MTS obtains it from the Directory using the Directory name. If the Directory name is omitted, the MTS does without it. If both are included, the MTS relies firstly upon the *OR-address*. Should it determine that the OR-address is invalid (e.g., obsolete), it proceeds as if the *OR-address* had been omitted, relying upon the Directory name.

At delivery the MTS includes an *OR-address* and possibly a Directory name in each OR-name it supplies to a message's recipient or to the originator of a report's subject message or probe. The Directory name is included if the originator supplied it or if it was specified as the member of an expanded DL.

NOTE – Redirection or DL expansion may cause the MTS to convey to a UA or MS at delivery, OR-names the UA or MS did not supply at direct submission.

For information relating to organisations which operate in more than one country, see annex G . See also 7.3.2 in ITU-T Rec. X.400 | ISO/IEC 10021-1.

18 Addressing

This clause specifies how users and DLs are addressed. It defines *OR-addresses*, describes the structure of the attribute lists from which they are constructed, discusses the character sets from which individual *attributes* are composed, gives rules for determining that two *attribute lists* are equivalent and for the inclusion of conditional *attributes* in such lists, and defines the *standard attributes* that may appear in them.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

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

18.1 Attribute Lists

The *OR-addresses* of both users and DLs are attribute lists. An attribute list is an ordered set of *attributes*.

An attribute is an information item that describes a user or DL and that may also locate it in relation to the physical or organizational structure of the MHS (or the network underlying it).

An attribute has the following parts:

a) attribute type (or type): An identifier that denotes a class of information (e.g., personal names).

b) attribute value (or value): An instance of the class of information the attribute type denotes (e.g., a particular personal name).

Attributes are of the following two kinds:

a) standard attribute: An attribute whose type is bound to a class of information by this Specification.

   The value of every standard attribute except *terminal type* is either a string or a collection of strings.

b) domain-defined attribute: An attribute whose type is bound to a class of information by an MD. Thus the type and value of a domain-defined-attribute are defined by an MD; the MD is identified by a *private-domain-name*, or an *administration-domain-name*, or both.

   Both the type and value of every domain-defined attribute are strings.

NOTE – The widespread use of standard attributes produces more uniform and thus more user-friendly OR-addresses. However, it is anticipated that not all MDs will be able to employ such attributes immediately. The purpose of domain-defined attributes is to permit an MD to retain its existing, native addressing conventions for a time. It is intended, however, that all MDs migrate toward the use of standard attributes, and that domain-defined attributes be used only for an interim period.

18.2 Character Sets

Standard attribute values and domain-defined attribute types and values are constructed from Numeric, Printable, Teletex, and Universal Strings as follows:

a) The type or value of a particular domain-defined attribute may be a Printable String, a Teletex String, a Universal String, or any combination of these. The same choice (or choices) shall be made for both the type and value.

b) The kinds of strings from which standard attribute values may be constructed and the manner of construction (e.g., as one string or several) vary from one attribute to another (see 18.3).

The value of an attribute comprises strings of one of the following sets of varieties depending upon its type: Numeric only; Printable only; Numeric and Printable; and Printable, Teletex and Universal. With respect to this, the following rules govern each instance of communication:

a) For *administration-domain-name*, *private-domain-name*, and *postal-code* the same numeric value may be represented as either a Numeric or Printable String.

b) Wherever both Printable and Teletex Strings are permitted, strings of either or both varieties may be supplied. If both Printable and Teletex Strings are supplied, the two should unambiguously identify the same user.

c) Wherever Printable, Teletex and Universal strings are permitted, one, two or all three varieties may be supplied. Where more than one variety is supplied for an attribute, each value should unambiguously identify the same user. Many systems will not be able to render all possible characters that can be represented by Universal Strings (for example, being restricted to that subset of Universal String that supports national requirements), and some systems will be unable to render Universal Strings at all. Hence Universal Strings alone should only be used where it is known that all likely recipients can handle the characters concerned (e.g. within a national or regional community of users).

Where a Universal String is supplied, a language code as defined in ISO 639 may be added to facilitate the rendering of the Universal String; for example where a character is rendered differently in different languages, this may cause selection of an appropriate font. The language code comprises a two-character code specified by ISO 639, optionally followed by a space and a two-character ISO 3166 country code (see 4.4 in ISO 639) if it is necessary to identify a specific national usage of the language (e.g. "en" identifies the English language, "en GB" identifies English as used in the UK, and "en US" identifies English as used in the USA).

--`,,`-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

Where a Universal String contains characters only from the Basic Multilingual Plane (see ISO/IEC 10646-1), it may be encoded in ASN.1 either as a UniversalString or as a BMPString.

When comparing values of OR-address, any language codes that are present shall be disregarded.

ITU-T only:

The length of each string and of each sequence of strings in an attribute shall be limited as indicated in the more detailed (i.e., ASN.1) specification of attributes in ITU-T Rec. X.411.

NOTE 1 – Universal and Teletex Strings are permitted in attribute values to allow inclusion, e.g., of the accented characters commonly used in many countries.

NOTE 2 – The downgrading rules in annex B of ITU-T Rec. X.419 | ISO/IEC 10021-6 state that an OR-address cannot be downgraded if only a Universal String or a Teletex String (or both) has been supplied which contains characters that lie outside the Printable String repertoire.

NOTE 3 – ASN.1 permits the encoding of Teletex Strings using (amongst others) character repertoires 102, 103, 6 and 156; these provide two alternative encodings of many Latin characters. For compatibility with earlier systems, it is recommended that any characters from repertoires 102 and 103 are always encoded using these repertoires, and that repertoires 6 and 156 are not used when encoding a string which contains only characters available in repertoires 102 and 103. This applies to all instances of Teletex Strings in the MHS protocols.

18.3 Standard Attributes

The standard attribute types are listed in the first column of Table 9. For each listed type, the second column indicates the character sets--numeric, printable, teletex, and universal --from which attribute values may be drawn.

The table has three sections. Attribute types in the first are of a general nature, those in the second have to do with *routing to* a PDS, and those in the third have to do with *addressing within* a PDS.

Table 9 – Standard Attributes

Standard Attribute Type	Character Sets		
	Numeric	**Printable**	**Universal or Teletex**
General			
administration-domain-name	x	x	–
common-name	–	x	x
country-name	x	x	–
network-address	x*	–	–
numeric-user-identifier	x	–	–
organization-name	–	x	x
organizational-unit-names	–	x	x
personal-name	–	x	x
private-domain-name	x	x	–
terminal-identifier	–	x	–
terminal-type	–	–	–
Postal Routing			
pds-name	–	x	–
physical-delivery-country-name	x	x	–
postal-code	x	x	–
Postal Addressing			
extension-postal-OR-address-components	–	x	x
extension-physical-delivery-address-components	–	x	x
local-postal-attributes	–	x	x
physical-delivery-office-name	–	x	x
physical-delivery-office-number	–	x	x
physical-delivery-organization-name	–	x	x
physical-delivery-personal-name	–	x	x

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

Table 9 – Standard Attributes

Standard Attribute Type	Character Sets		
	Numeric	Printable	Universal or Teletex
post-office-box-address	–	x	x
poste-restante-address	–	x	x
street-address	–	x	x
unformatted-postal-address	–	x	x
unique-postal-name	–	x	x
Legend X permitted * Under prescribed circumstances a Sequence of Octet Strings			

The standard attribute types, summarized in the table, are individually defined and described in the subclauses below.

18.3.1 Administration-domain-name

An administration-domain-name is a standard attribute that identifies an ADMD relative to the country denoted by a *country-name*.

The value of an administration-domain-name is a Numeric or Printable String chosen from a set of such strings that is administered for this purpose by the country alluded to above.

NOTE – The attribute value comprising a single space (" ") shall be reserved for the following purpose. If permitted by the country denoted by the country-name attribute, a single space shall designate any (i.e., all) ADMDs within the country. This affects both the identification of users within the country and the routing of messages, probes, and reports to and among the ADMDs of that country. Regarding the former, it requires that the OR-addresses of users within the country be chosen so as to ensure their unambiguousness, even in the absence of the actual names of the users' ADMDs. Regarding the latter, it permits both PRMDs within, and ADMDs outside of the country, to route messages, probes, and reports to any of the ADMDs within the country, and requires that the ADMDs within the country interconnect themselves in such a way that the messages, probes, and reports are conveyed to their destinations.

[|The attribute value comprising a single zero ("0"), encoded as either a Printable or Numeric String, shall be reserved for use by PRMDs which are not connected to any ADMD and are not reachable from any ADMD. The single zero value shall not be used by a PRMD which is connected to one or more ADMDs. The single zero value shall not be used by a PRMD indirectly connected to an ADMD (i.e., where agreements exist with both an ADMD and intermediate PRMDs to route messages indirectly between the ADMD and the subject PRMD). In addition to providing an appropriate part of the OR-address space for such PRMDs, the single zero value enables ADMDs and other PRMDs (without routing agreements with the subject PRMD) to determine that messages, probes and reports cannot be routed to the subject PRMD. The presence of an OR-address with a single zero administration-domain-name in recipients for which responsibility is set to not-responsible, or in the originator of a message or report which has been DL-expanded or Redirected, or elsewhere, is legitimate and should not cause non-delivery.

NOTE – The single zero administration-domain-name does not require an implementation to take any special action, but it permits an implementation to save transmission costs by detecting that delivery will not be possible at an earlier stage than might otherwise be possible.

18.3.2 Common-name

A common-name is a standard attribute that identifies a user or DL relative to the entity denoted by another attribute (e.g., an *organization-name*).

The value of a common-name is a Printable String, Teletex String, Universal String, or a combination of these types. Whichever string type is used, the value is chosen from a set of such strings that is administered for this purpose (and perhaps others) by the entity alluded to above.

NOTE – Among many other possibilities, a common-name might identify an organizational role (e.g., "Director of Marketing").

18.3.3 Country-name

A country-name is a standard attribute that identifies a country (or, exceptionally, an International MD Registration Authority).

The value of a country-name is a Printable String that gives the character pair assigned to the country by ISO 3166, or a Numeric String that gives one of the numbers assigned to the country (or geographical area, or non-zoned service) by CCITT Rec. X.121.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

The Printable String attribute value comprising the characters "XX" shall be reserved to denote the International Registration Authority for Management Domain Names operated in accordance with ITU-T Rec. X.666 | ISO/IEC 9834-7.

NOTE 1 – The value "XX" is amongst those reserved in ISO 3166 for use by users of that standard; thus there is no possibility of a future clash between a new country code allocated in ISO 3166 and this reserved value.

NOTE 2 – There are some users who have employed the value "WW" as a country-name to achieve a similar effect to the value "XX" prior to the existence of a formal registration process. However, ISO 3166 has not currently assigned the value "WW" for this purpose.

18.3.4 Extension-postal-OR-address-components

An is a standard attribute that provides, in a postal address, additional information necessary to identify the addressee (e.g., an organizational unit).

The value of an extension-postal-OR-address-components is a Printable String, Teletex String, Universal String, or a combination of these types.

18.3.5 Extension-physical-delivery-address-components

An is a standard attribute that specifies, in a postal address, additional information necessary to identify the exact point of delivery (e.g., room and floor numbers in a large building).

The value of an extension-physical-delivery-address-components is a Printable String, Teletex String, Universal String, or a combination of these types.

18.3.6 Local-postal-attributes

A local-postal-attributes is a standard attribute that identifies the locus of distribution, other than that denoted by a physical-delivery-office-name attribute (e.g., a geographical area), of a user's physical messages.

The value of a local-postal-attributes is a Printable String, Teletex String, Universal String, or a combination of these types.

18.3.7 Network-address

A network-address is a standard attribute that gives the network address of a terminal.

The value of a network-address is any one of the following:

a) A Numeric String governed by CCITT Rec. X.121.

b) Two Numeric Strings governed by CCITT Rec. E.164.

c) A PSAP address.

NOTE 1 – Among the strings admitted by CCITT Rec. X.121 are Telex and Telephone numbers preceded by an escape digit.

NOTE 2 – The MHS protocols allow for 16 digits to be carried in the X.121 address component of network-address. This permits the use of an escape digit plus a full 15-digit telephone or ISDN number. Other protocols may have a limit of 14 digits, or a different mechanism for encoding of 15-digit numbers; mapping between MHS and such protocols, if required, is a local matter.

18.3.8 Numeric-user-identifier

A numeric-user-identifier is a standard attribute that numerically identifies a user relative to the MD denoted by a *private-domain-name*, or an administration-domain-name, or both.

The value of a numeric-user-identifier is a Numeric String chosen from a set of such strings that is administered for this purpose by the MD alluded to above.

18.3.9 Organization-name

An organization-name is a standard attribute that identifies an organization. The value of an organization-name is a Printable String, Teletex String, Universal String, or a combination of these types.

When used in a *mnemonic OR-address* (see 18.5.1), as a national matter organizations may be identified either relative to the country denoted by a country-name (so that organization names are unique within the country); or relative to the MD identified by a *private-domain-name*, or an administration-domain-name, or both. Whichever string type is used, the string is chosen from a set of such strings that is administered for this purpose (and perhaps others) by the country or MD alluded to above.

NOTE – In countries choosing country-wide unique organization-names, a national registration authority for organization-names is required.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

When used in a *terminal OR-address* (see 18.5.4), the organization-name is a free-form value, with no requirement for registration.

18.3.10 Organizational-unit-names

An organizational-unit-names is a standard attribute that identifies one or more units (e.g., divisions or departments) of the organization denoted by an organization-name, each unit but the first being a sub-unit of the units whose names precede it in the attribute.

The value of an organizational-unit-names is an ordered sequence of Printable Strings, an ordered sequence of Teletex Strings, an ordered sequence of Universal Strings, or any combination of these three options. Whichever string type is used, each string is chosen from a set of such strings that is administered for this purpose (and perhaps others) by the organization (or encompassing unit) alluded to above.

18.3.11 Pds-name

A pds-name is a standard attribute that identifies a PDS relative to the MD denoted by a *private-domain-name*, or an administration-domain-name, or both.

The value of a pds-name is a Printable String chosen from a set of such strings that is administered for this purpose by the MD alluded to above.

18.3.12 Personal-name

A personal-name is a standard attribute that identifies a person relative to the entity denoted by another attribute (e.g., an organization-name).

The value of a personal-name comprises the following four pieces of information, the first mandatory, the others optional:

a) The person's surname.

b) The person's given name.

c) The initials of all of his names but his surname.

d) His generation (e.g., "Jr").

The above information is supplied as Printable Strings, Teletex Strings, Universal Strings, or any combination of these types.

18.3.13 Physical-delivery-country-name

A physical-delivery-country-name is a standard attribute that identifies the country in which a user takes delivery of physical messages.

The value of a physical-delivery-country-name is subject to the same constraints as is the value of a country-name.

18.3.14 Physical-delivery-office-name

A physical-delivery-office-name is a standard attribute that identifies the city, village, etc. in which is situated the post office through which a user takes delivery of physical messages.

The value of a physical-delivery-office-name is a Printable String, Teletex String, Universal String, or a combination of these types.

18.3.15 Physical-delivery-office-number

A physical-delivery-office-number is a standard attribute that distinguishes among several post offices denoted by a single physical-delivery-office-name.

The value of a physical-delivery-office-number is a Printable String, Teletex String, Universal String, or a combination of these types.

18.3.16 Physical-delivery-organization-name

A physical-delivery-organization-name is a standard attribute that identifies a postal patron's organization.

The value of a physical-delivery-organization-name is a Printable String, Teletex String, Universal String, or a combination of these types.

18.3.17 Physical-delivery-personal-name

A physical-delivery-personal-name is a standard attribute that identifies a postal patron.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

The value of a physical-delivery-personal-name is a Printable String, Teletex String, Universal String, or a combination of these types.

18.3.18 Post-office-box-address

A post-office-box-address is a standard attribute that specifies the number of the post office box by means of which a user takes delivery of physical messages.

The value of a post-office-box-address is a Printable String, Teletex String, Universal String, or a combination of these types chosen from the set of such strings assigned for this purpose by the post office denoted by a physical-delivery-office-name attribute.

18.3.19 Postal-code

A postal-code is a standard attribute that specifies the postal code for the geographical area in which a user takes delivery of physical messages.

The value of a postal-code is a Numeric or Printable String chosen from the set of such strings that is maintained and standardized for this purpose by the postal administration of the country identified by a physical-delivery-country-name attribute.

18.3.20 Poste-restante-address

A poste-restante-address is a standard attribute that specifies the code that a user gives to a post office in order to collect the physical messages that await delivery to him.

The value of a poste-restante-address is a Printable String, Teletex String, Universal String, or a combination of these types.

18.3.21 Private-domain-name

A private-domain-name is a standard attribute that identifies a PRMD. As a national matter, this identification may be either relative to the country denoted by a country-name (so that PRMD names are unique within the country), or relative to the ADMD identified by an administration-domain-name.

The value of a private-domain-name is a Numeric or Printable String chosen from a set of such strings that is administered for this purpose by the country or ADMD alluded to above.

NOTE – In countries choosing country-wide unique PRMD names, a national registration authority for private-domain-names is required.

18.3.22 Street-address

A street-address is a standard attribute that specifies the street address (e.g., house number and street name and type (e.g., "Road")) at which a user takes delivery of physical messages.

The value of a street-address is a Printable String, Teletex String, Universal String, or a combination of these types.

18.3.23 Terminal-identifier

A terminal-identifier is a standard attribute that gives the terminal identifier of a terminal (e.g., a Telex answer back or a Teletex terminal identifier).

The value of a terminal-identifier is a Printable String.

18.3.24 Terminal-type

A terminal-type is a standard attribute that gives the type of a terminal.

The value of a terminal-type is any one of the following: *Telex*, *Teletex*, *G3 facsimile*, *G4 facsimile*, *IA5 terminal*, and *Videotex*.

18.3.25 Unformatted-postal-address

An unformatted-postal-address is a standard attribute that specifies a user's postal address in free form.

The value of an unformatted-postal-address is a sequence of Printable Strings, each representing a line of text; a single Universal String or Teletex String, lines being separated by CR LF or LF CR (a maximum of five occurrences of the separator is allowed); or both.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

18.3.26 Unique-postal-name

A unique-postal-name is a standard attribute that identifies the point of delivery, other than that denoted by a street-address, post-office-box-address, or poste-restante-address, (e.g., a building or hamlet) of a user's physical messages.

The value of a unique-postal-name is a Printable String, Teletex String, Universal String, or a combination of these types.

18.4 Attribute List Equivalence

Several OR-addresses, and thus several attribute lists, may denote the same user or DL. This multiplicity of OR-addresses results in part (but not in full) from the following attribute list equivalence rules:

a) The relative order of standard attributes is insignificant.

b) Where the value of a standard attribute may be a Numeric String or an equivalent Printable String, the choice between them shall be considered insignificant.

NOTE – This rule applies even to the country-name standard attribute, where the choice between X.121 or ISO 3166 forms shall be considered insignificant. Where X.121 allocates more than one number to a country the significance of which number is used has not been standardised by this Specification.

c) Where the value of a standard attribute may be a Printable String, Teletex String, Universal String, or a combination of these types, the choice between the seven possibilities shall be considered insignificant.

d) Where the type or value of a domain-defined attribute, or the value of a standard attribute, comprises characters from the Printable String repertoire, the choice where permitted between encoding it in a Universal String or Teletex String and in a Printable String shall be considered insignificant.

e) Where the type or value of a domain-defined attribute, or the value of a standard attribute, comprises characters from the Teletex String repertoire, the choice where permitted between encoding it in a Teletex String and in a Universal String shall be considered insignificant.

f) Where the value of a standard attribute may contain letters, the cases of those letter shall be considered insignificant.

g) In a domain-defined attribute type or value, or in a standard attribute value, all leading, all trailing, and all but one consecutive embedded spaces shall be considered insignificant.

h) In a Teletex String, the Non-spacing underline graphic character shall be considered insignificant, as shall all control functions except Space and those used for code extension procedures.

i) In a Teletex String, the choice between different encodings of the same character shall be considered insignificant.

j) In a Universal String, the choice between different encodings of the same character (for example, the order in which the components of composing characters are encoded) shall be considered insignificant.

NOTE – An MD may impose additional equivalence rules upon the attributes it assigns to its own users and DLs. It might define, e.g., rules concerning punctuation characters in attribute values, the case of letters in such values, or the relative order of domain-defined attributes.

18.5 OR-Address Forms

Every user or DL is assigned one or more OR-addresses. An OR-address is an attribute list that distinguishes one user from another and identifies the user's point of access to the MHS or the DL's expansion point.

An OR-address may take any of the forms summarized in Table 10. The first column of the table identifies the attributes available for the construction of OR-addresses. For each OR-address form, the second column indicates the attributes that may appear in such OR-addresses and their grades (see also 18.6).

The table has four sections. Attribute types in the first are those of a general nature. Attribute types in the second and third those specific to physical delivery, but unformatted-postal-address may be used as an extension to the terminal address. The fourth section encompasses domain-defined attributes.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

Table 10 – Forms of OR-Address

Attribute Type	OR-Address Forms				
			POST		
	MNEM	NUMR	F	U	TERM
- General -					
administration-domain-name	M	M	M	M	C
common-name	C	–	–	–	C*
country-name	M	M	M	M	C
network-address	–	–	–	–	M
numeric-user-identifier	–	M	–	–	–
organization-name	C	–	–	–	C*
organizational-unit-names	C	–	–	–	C*
personal-name	C	–	–	–	C*
private-domain-name	C	C	C	C	C
terminal-identifier	–	–	–	–	C
terminal-type	–	–	–	–	C
- Postal Routing -					
pds-name	–	–	C	C	–
physical-delivery-country-name	–	–	M	M	–
postal-code	–	–	M	M	–
- Postal Addressing -					
extension-postal -OR-address-components	–	–	C	–	–
extension-physical-delivery -address-components	–	–	C	–	–
local-postal-attributes	–	–	C	–	–
physical-delivery-office-name	–	–	C	–	–
physical-delivery-office-number	–	–	C	–	–
physical-delivery-organization-name	–	–	C	–	–
physical-delivery-personal-name	–	–	C	–	–
post-office-box-address	–	–	C	–	–
poste-restante-address	–	–	C	–	–
street-address	–	–	C	–	–
unformatted-postal-address	–	–	–	M	C*
unique-postal-name	–	–	C	–	–
- Domain-defined -					
domain-defined (one or more)	C	C	–	–	C

- Legend -

MNEM mnemonic NUMR numeric POST postal TERM terminal
F formatted U unformatted M mandatory C conditional
C* conditional, but intended to be used for rendition purposes and not for MHS addressing or routing

The forms of OR-address, summarized in the table, are individually defined and described in the subclauses below. The representation of OR-addresses for human usage is described in Annex F.

18.5.1 Mnemonic OR-Address

A mnemonic OR-address is one that provides a memorable identification for a user or DL. It identifies an MD, and a user or DL relative to it.

A mnemonic OR-address comprises the following attributes:

a) One country-name, one administration-domain-name and conditionally one private-domain-name, which together identify an MD.

b) One organization-name, or one organizational-unit-names, or one personal-name, or one common-name, or one or more domain-defined attributes, or a combination of the above, which together identify a user or DL relative to the MD in item *a* above. If organizational-unit-names is present, then organization-name shall be present.

18.5.2 Numeric OR-Address

A numeric OR-address is one that numerically identifies a user relative to an MD.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

A numeric OR-address comprises the following attributes:

a) One country-name, one administration-domain-name and conditionally one private-domain-name, which together identify an MD.

b) One numeric-user-identifier which identifies the user relative to the MD in item *a* above.

c) Conditionally, one or more domain-defined attributes which provide information additional to that which identifies the user.

NOTE – Only the numeric-user-identifier is restricted to be numeric.

18.5.3 Postal OR-Address

A postal OR-address is one that identifies a user by means of its postal address. It identifies the PDS through which the user is to be accessed and gives the user's postal address.

The following kinds of postal OR-address are distinguished:

a) formatted: Said of a postal OR-address that specifies a user's postal address by means of several attributes. For this form of postal OR-address, this Specification prescribes the structure of postal addresses in some detail.

b) unformatted: Said of a postal OR-address that specifies a user's postal address in a single attribute. For this form of postal OR-address, this Specification largely does not prescribe the structure of postal addresses.

A postal OR-address, whether formatted or unformatted, comprises the following attributes:

a) One country-name, one administration-domain-name and conditionally one private-domain-name, which together identify an MD.

b) Conditionally, one pds-name which identifies the PDS by means of which the user is to be accessed.

c) One physical-delivery-country-name and one postal-code, which together identify the geographical region in which the user takes delivery of physical messages.

A formatted postal OR-address comprises, additionally, one of each of those conditional postal addressing attributes listed in Table 10 that are required by the PDS. A formatted postal OR-address does not contain the unformatted-postal-address attribute.

An unformatted postal OR-address comprises, additionally, one unformatted-postal-address attribute.

NOTE – The total number of characters in the values of all attributes but country-name, administration-domain-name, and pds-name in a postal OR-address should be small enough to permit their rendition in 6 lines of 30 characters, the size of a typical physical envelope window. The rendition algorithm is PDAU-specific but is likely to include inserting delimiters (e.g., spaces) between some attribute values.

18.5.4 Terminal OR-Address

A terminal OR-address is one that identifies a user by means of the network address and, if required, the type of his terminal. It may also identify the MD through which that terminal is accessed. In the case of a Telematic terminal, it gives the terminal's network address and possibly its terminal identifier and terminal type. In the case of a Telex terminal, it gives its Telex number.

A terminal OR-address comprises the following attributes:

a) One network-address.

b) Conditionally, one terminal-identifier.

c) Conditionally, one terminal-type.

d) Conditionally, both one country-name and one administration-domain-name and conditionally one private-domain-name which together identify an MD.

e) Conditionally, one or more attributes chosen from organization-name, organizational-unit-names, personal-name, unformatted-postal-address and common-name, and conditionally one or more domain-defined attributes, all of which provide additional information to identify the user.

The private-domain-name and the domain-defined attributes shall be present only if the country-name and administration-domain-name attributes are present.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

18.5.5 Determination of Address Forms

The form of an OR-address shall be determined as follows:

if it contains a numeric-user-identifier, it is a numeric OR-address;

if it contains a network-address, it is a terminal OR-address;

if it contains a physical-delivery-country, it is a postal OR-address;

any other OR-address is a mnemonic OR-address.

If a postal OR-address contains an unformatted-postal-address it is an unformatted postal OR-address, otherwise it is a formatted postal OR-address.

18.6 Conditional Attributes

The presence or absence in a particular OR-address of the attributes marked conditional in Table 10 is determined as follows.

All conditional attributes except those specific to postal OR-addresses are present in an OR-address at the discretion of, and in accordance with rules established by, the MD denoted by the country-name, administration-domain-name and, if present, private-domain-name attributes.

All conditional attributes specific to postal OR-addresses are present or absent in such OR-addresses so as to satisfy the postal addressing requirements of the users they identify.

19 Routing

ITU-T version:

To convey a message, probe, or report toward a user or the expansion point of a DL, an MTA must not only locate the user or DL (i.e., obtain its OR-address) but also select a route to that location.

External routing is an incremental and only loosely standardized process. Suggested below are several principles of external routing. Internal routing is outside the scope of this Recommendation.

The following principles are illustrative, not definitive:

a) In an MHS that comprises a single MD, of course, routing is not an issue.

b) A PRMD may be connected to a single, ADMD. When this is so, routing always involves the ADMD necessarily.

c) An ADMD may be connected to multiple PRMDs. When this is so, routing may be based upon conditional OR-address attributes, including but not limited to private-domain-name.

d) An MD may be directly connected to some but not all other MDs. When the OR-address identifies a MD to which no direct connection exists, routing may be based upon bilateral agreement with the MDs to which direct connections do exist and other local rules.

e) When the MD is directly connected to the MD identified by the OR-address, the object is typically routed to that MD directly.

f) By bilateral agreement, one MD might route an object to another MD for the purpose, e.g., of conversion.

g) An MD may route to a malformed OR-address provided (of course) that it contains at least the attributes required to do so.

NOTE – The bilateral agreements and local rules alluded to above are beyond the scope of this Recommendation and may be based upon technical, policy, economic, or other considerations.

ISO/IEC version:

To convey a message, probe, or report toward a user or the expansion point of a DL, an MTA must not only locate the user or DL (i.e., obtain its OR-address) but also select a route to that location. Routing is thus the process of selecting, given an OR-address, the MTA to which the message, probe or report should be transferred.

This clause is tutorial in nature: ITU-T Rec. X.412 | ISO/IEC 10021-10 standardises mechanisms for dissemination of and use of the information required for routing decisions; ITU-T Rec. X.404 | ISO/IEC TR 10021-11 gives advice to messaging system managers on use of these routing mechanisms.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

Where no other considerations apply, the optimal routing is to transfer the message as directly as possible to the MTA to which the recipient's UA is connected. However, there may be factors making a more indirect route appropriate such as: less direct routes utilising higher bandwidth links between MTAs; using late fan-out to give optimisation of transmission costs; and needing to access an intermediate MTA for a service such as conversion. The costs of disseminating and storing routing information possibly combined with the undesirability for some domains of disclosing internal structure means that frequently routing directly to the ultimate MTA will not be possible, even when desirable.

The first part of the routing decision that an MTA must make is whether this recipient is in its own MD. To do this, the MTA must know all the combinations of country-name, administration-domain-name and private-domain-name attributes which identify its own domain. A PRMD may have as many combinations of these as there are entry points from ADMDs to that PRMD, although for PRMDs existing entirely within countries adopting nationally unique private-domain-names a single pair of values of country-name and private-domain-name attributes will be sufficient to identify that PRMD internally regardless of whether or not semantic absence of the administration-domain-name is permitted at entry points from ADMDs.

If the recipient is identified as within the same MD the values of other attributes of the recipient's OR-address are examined to determine whether the recipient is a UA served by that MTA, in which case local delivery will occur, or whether an appropriate MTA within the MD can be identified to which the message can be relayed. Failing either of these, a non-delivery event must occur.

Not all MTAs within an MD necessarily need be configured with the capability to relay to or receive from other MDs, but there must be at least one MTA within the MD with such capabilities if the MD is not to remain isolated from all other MDs. Every MTA within a (non-isolated) MD must be capable of routing to an MTA within that MD which can relay to other MDs, if not possessing this capability itself. So, even if the recipient is identified as being outside the MD, relaying to another MTA within the MD may still be necessary.

If the external MD is identified as one to which a direct connection exists, then this direct connection will often be used. The external MD may also be identified as one reached by relaying through one or more intermediate MD. If these intermediate MDs are PRMDs then this option can only be exercised by bilateral agreement. Alternatively, the external MD may be unknown and then the services of an ADMD will be required.

The role of an ADMD within the MHS is to provide, directly or indirectly, relaying to all other ADMDs, and to relay messages to all PRMDs directly connected to that ADMD. Thus a PRMD always has the option of choosing to use the services of an ADMD for routing to other PRMDs.

When more than one entry point to an external MD can be identified, additional OR-address attributes or other considerations may be used to determine the most appropriate entry point. In the extreme case of the originating MD having complete information about the recipient's MD this would allow direct communication between originator's MTA and recipient's MTA.**]**

SECTION 5 – USE OF THE DIRECTORY

20 Overview

This section describes the uses to which the MHS may put the Directory if it is present. If the Directory is unavailable to the MHS, how, if at all, the MHS performs these same tasks is a local matter.

This section covers the following topics:

a) Authentication;

b) Name resolution;

c) DL expansion;

d) Capability assessment.

21 Authentication

A functional object may accomplish authentication using information stored in the Directory.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

22 Name Resolution

A functional object may accomplish name resolution using the Directory.

To obtain the OR-address(es) of a user or DL whose Directory name it possesses, an object presents that name to the Directory and requests from the Directory entry the following attributes:

a) *MHS OR-Addresses*.

b) *Preferred Delivery Methods*.

To do this successfully, the object must first authenticate itself to the Directory and have access rights to the information requested.

The functional object then attempts to determine an OR-address which satisfies a preferred delivery method. For methods other than mhs-delivery the functional object may need to construct an address using other attributes from the directory entry and local configuration information.

23 DL Expansion

A functional object may accomplish DL expansion using the Directory, first verifying that the necessary submit permissions exist.

The object presents the Directory name of a DL to the Directory and requests from the Directory entry the following attributes:

a) *MHS DL Members*.

b) *MHS DL Policy.*

c) *MHS DL Submit Permissions.*

To do this successfully, the MTA must first authenticate itself to the Directory and have access rights to the information requested.

24 Capability Assessment

A functional object may assess the capabilities of a user, DL or MS using the Directory.

The following Directory attributes represent user capabilities of possible significance in Message Handling:

a) *MHS Deliverable Content Types*.

b) *MHS Deliverable EITs.*

c) *MHS Maximum Content Length.*

d) *MHS OR-Addresses with Capabilities.*

e) *MHS Undeliverable EITs.*

f) *Preferred Delivery Methods*

The following Directory attributes represent MS capabilities of possible significance in Message Handling:

a) *MHS Supported Attributes*.

b) *MHS Supported Automatic Actions.*

c) *MHS Supported Content Type.s*

d) *MHS Supported Matching Rules.*

To assess a particular capability of a user, DL or MS whose Directory name it possesses, the object presents that name to the Directory and requests from the Directory entry the attribute associated with that capability.

To do this successfully, the MTA must first authenticate itself to the Directory and have access rights to the information requested.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

SECTION 6 – OSI REALIZATION

25 Overview

This section describes how the MHS is realized by means of OSI.

This section covers the following topics:

a) Application service elements;

b) Application contexts.

26 Application Service Elements

This clause identifies the application service elements (ASEs) that figure in the OSI realization of Message Handling.

In OSI the communication capabilities of open systems are organized into groups of related capabilities called ASEs. The present clause reviews this concept from the OSI Reference Model, draws a distinction between *symmetric* and a*symmetric* ASEs, and introduces the ASEs defined for or supportive of Message Handling.

NOTE – Besides the ASEs discussed, the MHS relies upon the Directory Access Service Element defined in ITU-T Rec. X.519 | ISO/IEC 9594-6. However, since that ASE does not figure in the *ACs* for Message Handling (see ITU-T Rec. X.419 | ISO/IEC 10021-6), it is not discussed here.

26.1 The ASE Concept

The ASE concept is illustrated in Figure 12, which depicts two communicating open systems. Only the OSI-related portions of the open systems, called AEs, are shown. Each AE comprises a UE and one or more ASEs. A UE represents the controlling or organizing portion of an AE which defines the open system's role (e.g., that of an MTA). An ASE represents one of the communication capability sets, or services (e.g., for message submission or transfer), that the UE requires to play its role.

The relationship between two AEs in different open systems is called an application association. The ASEs in each open system communicate with their peer ASEs in the other open system via a presentation connection between them. That communication is what creates and sustains the relationship embodied in the application association. For several ASEs to be successfully combined in a single AE, they must be designed to coordinate their use of the application association.

An ASE plays the largely mechanical role of translating requests and responses made by its UE to and from the form dictated by the application protocol that governs the ASE's interaction with its peer ASE in the open system to which the association connects it. The ASE realizes an abstract service, or a part thereof, for purposes of OSI communication (see clauses 28-30).

NOTE – Strictly speaking, an open system's role is determined by the behaviour of its application processes. In the Message Handling context an application process realizes a functional object of one of the types defined in clause 7. A UE in turn is one part of an application process.

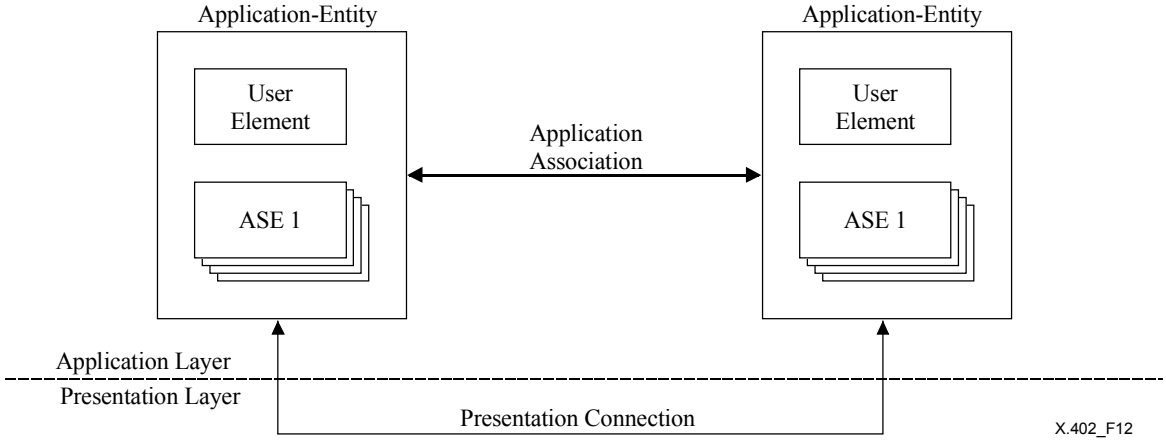


Figure 12 – The ASE Concept

--`,,`-`-`,,`,,`,`,,`---
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

26.2 Symmetric and Asymmetric ASEs

The following two kinds of ASE, illustrated in Figure 13, can be distinguished:

a) symmetric: Said of an ASE by means of which a UE both supplies and consumes a service. The ASE for message transfer, e.g., is symmetric because both open systems, each of which embodies an MTA, offer and may consume the service of message transfer by means of it.

b) asymmetric: Said of an ASE by means of which a UE supplies or consumes a service, but not both, depending upon how the ASE is configured. The ASE for message delivery, e.g., is asymmetric because only the open system embodying an MTA offers the associated service and only the other open system, which embodies a UA or MS, consumes it.

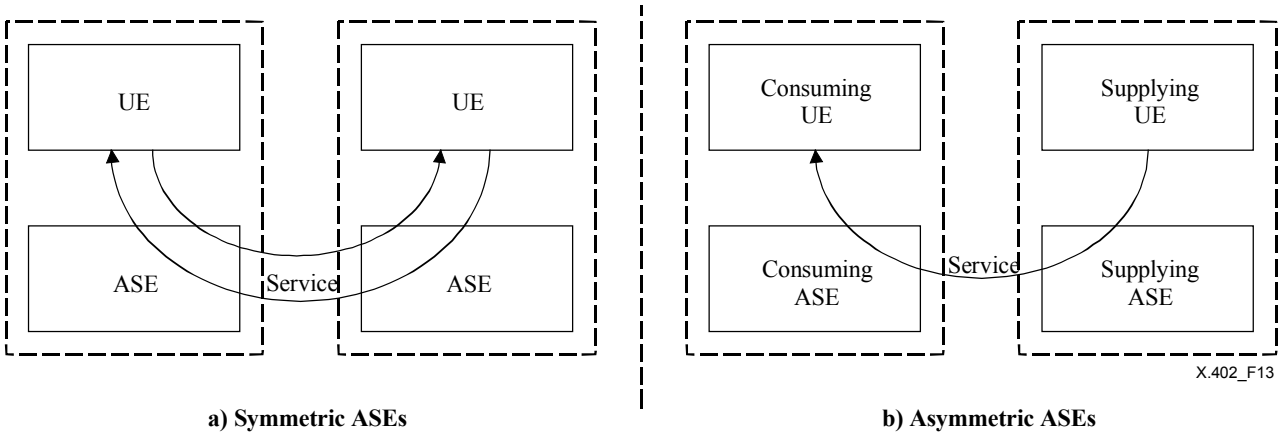


Figure 13 – Symmetric and Asymmetric ASEs

With respect to a particular asymmetric ASE, one UE supplies a service which the other consumes. The ASEs co-located with the UEs assist in the service's supply and consumption. The resulting four roles are captured in Figure 14 and in the following terminology:

a) *x*-supplying UE: An application process that supplies the service represented by asymmetric ASE *x*.

b) *x*-supplying ASE: An asymmetric ASE *x* configured for co-location with an *x* supplying-UE.

c) *x*-consuming UE: An application process that consumes the service represented by asymmetric ASE *x*.

d) *x*-consuming ASE: An asymmetric ASE *x* configured for co-location with an *x*-consuming-UE.

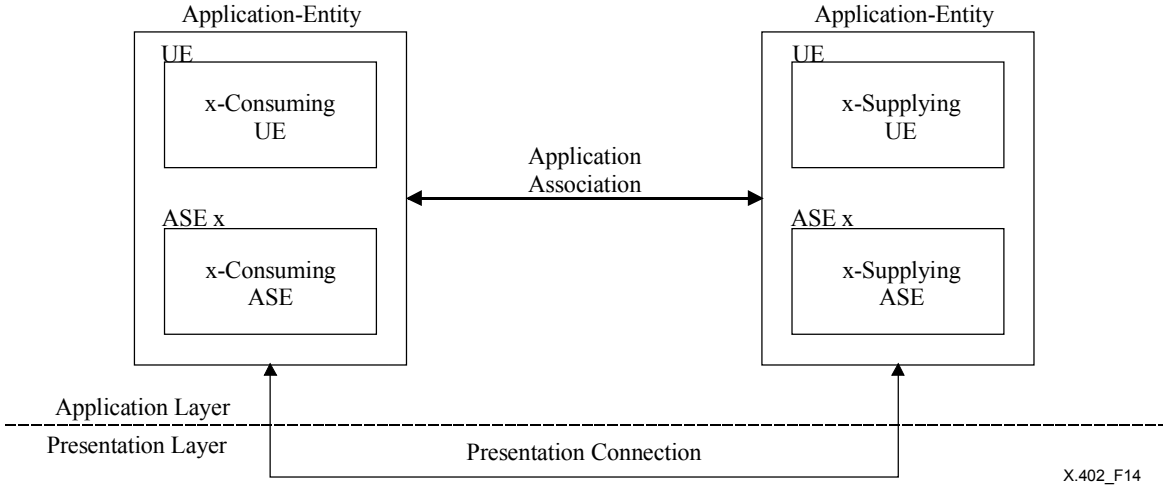


Figure 14 – Terminology for Asymmetric ASEs

As indicated, the four roles described above are defined relative to a particular ASE. When an AE comprises several asymmetric ASEs, these roles are assigned independently for each ASE. Thus, as shown in Figure 15, a single UE might serve as the consumer with respect to one ASE and as the supplier with respect to another.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

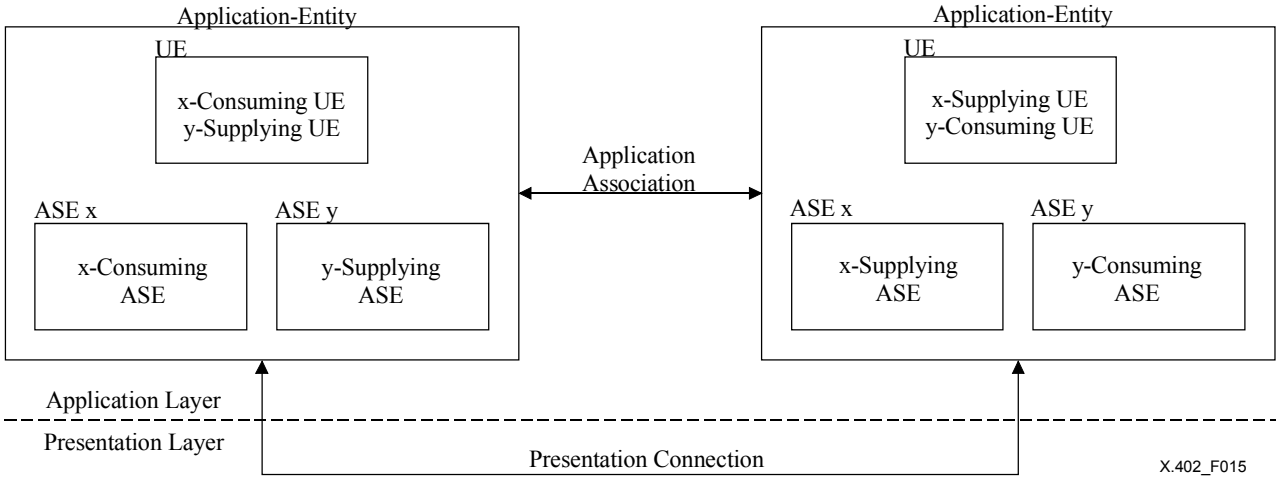


Figure 15 –Multiple Asymmetric ASEs

26.3 Message Handling ASEs

The ASEs that provide the various Message Handling services are listed in the first column of Table 11. For each ASE listed, the second column indicates whether it is symmetric or asymmetric. The third column identifies the functional objects--UAs, MSs, MTAs, and AUs--that are associated with the ASE, either as consumer or as supplier.

Table 11 – Message Handling ASEs

		Functional Objects			
ASE	Form	UA	MS	MTA	AU
MTSE	SY	–	–	CS	–
MSSE	ASY	C	CS	S	–
MDSE	ASY	C	C	S	–
MRSE	ASY	C	S	–	–
MASE	ASY	C	CS	S	–

Legend

SY	symmetric
ASY	asymmetric
C	consumer
S	supplier

The Message Handling ASEs, summarized in the table, are individually introduced in the subclauses below. Each is defined in ITU-T Rec. X.419 | ISO/IEC 10021-6.

26.3.1 Message Transfer

The Message Transfer Service Element (MTSE) is the means by which the transfer transmittal step is effected.

26.3.2 Message Submission

The Message Submission Service Element (MSSE) is the means by which the submission transmittal step is effected.

26.3.3 Message Delivery

The Message Delivery Service Element (MDSE) is the means by which the delivery transmittal step is effected.

26.3.4 Message Retrieval

The Message Retrieval Service Element (MRSE) is the means by which the retrieval transmittal step is effected.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

26.3.5 Message Administration

The Message Administration Service Element (MASE) is the means by which a UA, MS, or MTA places on file with one another information that enables and controls their subsequent interaction by means of the MSSE, MDSE, MRSE, and MASE.

26.4 Supporting ASEs

The general-purpose ASEs upon which Message Handling ASEs depend are listed in the first column of Table 12. For each listed ASE, the second column indicates whether it is symmetric or asymmetric.

Table 12 – Supporting ASEs

ASE	Form
ROSE	SY
RTSE	SY
ACSE	SY

Legend	
SY	symmetric
ASY	asymmetric

The supporting ASEs, summarized in the table, are individually introduced in the subclauses below.

26.4.1 Remote Operations

The Remote Operations Service Element (ROSE) is the means by which the asymmetric Message Handling ASEs structure their request-response interactions between consuming and supplying open systems.

The ROSE is defined in ITU-T Rec. X.880 | ISO/IEC 13712-1.

26.4.2 Reliable Transfer

The Reliable Transfer Service Element (RTSE) is the means by which various symmetric and asymmetric Message Handling ASEs convey information objects--especially large ones (e.g., facsimile messages)--between open systems so as to ensure their safe-storage at their destinations.

The RTSE is defined in ITU-T Rec. X.218 | ISO/IEC 9066-1.

26.4.3 Association Control

The Association Control Service Element (ACSE) is the means by which all application associations between open systems are established, released, and in other respects managed.

The ACSE is defined in ITU-T Rec. X.217 | ISO 8649.

27 Application Contexts

In OSI the communication capabilities (i.e., ASEs) of two open systems are marshalled for a particular purpose by means of application contexts (ACs). An AC is a detailed specification of the use of an association between two open systems, i.e., a protocol.

An AC specifies how the association is to be established (e.g., what initialization parameters are to be exchanged), what ASEs are to engage in peer-to-peer communication over the association, what constraints (if any) are to be imposed upon their individual use of the association, whether the initiator or responder is the consumer of each asymmetric ASE, and how the association is to be released (e.g., what finalization parameters are to be exchanged).

Every AC is named (by an ASN.1 Object Identifier). The initiator of an association indicates to the responder the AC that will govern the association's use by conveying the AC's name to it by means of the ACSE.

An AC also identifies by name (an ASN.1 Object Identifier) the abstract syntaxes of the APDUs that an association may carry as a result of its use by the AC's ASEs. Conventionally one assigns a name to the set of APDUs associated either

--`,,`-`-`,,`,,`,`,,`---
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

with each individual ASE or with the AC as a whole. The initiator of an association indicates to the responder the one or more abstract syntaxes associated with the AC by conveying their names to it via the ACSE.

The abstract syntax of an APDU is its structure as an information object (e.g., an ASN.1 Set comprising an Integer command code and an IA5 String command argument). It is distinguished from the APDU's transfer syntax which is how the information object is represented for transmission between two open systems (e.g., one octet denoting an ASN.1 Set, followed by one octet giving the length of the Set, etc.).

The ACs by means of which the various Message Handling services are provided are specified in ITU-T Rec. X.419 | ISO/IEC 10021-6. These protocols are known as P1, P3, and P7.

NOTE – The nature of a message's content does not enter into the definition of Message Handling ACs because the content is encapsulated (as an Octet String) in the protocols by means of which it is conveyed.

SECTION 7 – ABSTRACT SERVICE DEFINITION CONVENTIONS

28 Overview

When describing a complex distributed information processing task there is some advantage in specifying the task in abstract rather than concrete terms. This approach ensures that the task's functional requirements are stated independently of its concrete realization. As well as permitting the specification to develop by a process of step-wise refinement, this separation is important since each aspect of the task may admit of several concrete realizations. For example, in a Message Transfer System comprising three message transfer agents, the first and second might interact using OSI communication, and the second and third by proprietary means.

This section specifies the conventions for abstractly describing the services provided by an distributed information processing task, the abstract service, by means of an abstract model. The realization of the abstract service by means of OSI communication services is also described.

NOTE – This section replaces and makes obsolete the Abstract Service Definition Conventions in CCITT Rec. X.407 (1988) | ISO/IEC 10021-3: 1990.

ITU-T Rec. X.880 | ISO/IEC 13712-1 defines several information object classes that are useful in the specification of ROS-based application protocols such as those defined for MHS.

29 Components of the Abstract Model

29.1 Abstract Objects

An abstract object (MHS-object) is a functional entity, possibly one of several which interact with one another. An abstract object of one type might represent a system; multiple abstract objects of another type might represent its users. Abstract objects interact only when bound together in an association which defines the services offered and the context of their interaction in terms of an abstract contract.

An MHS-object is specified as an instance of the MHS-object information object class. Its definition is identical to the Remote Operations ROS-OBJECT-CLASS information object class. This defines the capabilities of an abstract object in terms of the (association) contracts it supports as initiator, or responder, or in either role.

```
MHS-OBJECT ::= ROS-OBJECT-CLASS
```

29.2 Abstract Contracts

An abstract contract (contract) defines a context within which a pair of abstract objects can interact. This includes a specification of the manner in which the two abstract objects establish an association (bind), release an association (unbind), and identifies the abstract ports bound together for the duration of the association. When specifying a contract, the ports in which the association initiator assumes the role of "consumer", the ports at which it assumes the role of "supplier", and the ports which are either symmetrical or in which the association initiator can occupy both the "consumer" and "supplier" roles are identified.

A contract is defined as an instance of the Remote Operations CONTRACT information object class.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

29.3 Connection Packages

A connection package specifies that part of a contract concerned with the dynamic establishment and release of an association. It specifies the abstract-bind operation used to establish, and the abstract-unbind operation used to release the association.

A connection-package is defined as an instance of the Remote Operations CONNECTION-PACKAGE information object class.

29.4 Abstract Ports

An abstract port (port) is a point at which an abstract object interacts with another abstract object when bound together under the terms of a contract. It defines the set of operations which may be invoked by an abstract object assuming the role of "consumer", the operations which may be invoked by an abstract object assuming the role of "supplier", and the operations which may be invoked by either abstract object.

A port is defined as symmetric if all instances of the port are identical (i.e. consumer and supplier roles are not distinguished). A port is defined as asymmetric if each instance of the port is of one of two kinds, supplier or consumer (i.e. the roles are distinguished).

A port is specified as an instance of the PORT information object class. Its definition is identical to the Remote Operations OPERATION-PACKAGE information object class.

```
PORT ::= OPERATION-PACKAGE
```

29.5 Abstract Operations and Abstract Errors

An abstract operation is a procedure that one abstract object (the invoker) can request of another (the performer) at a port pair bound within the terms of a contract. If the ports are symmetric, then either abstract object may invoke the operation. If the ports are asymmetric, then the port definition prescribes which operations may be invoked by the abstract object acting as the consumer of the port, and which may be invoked by that acting as the supplier.

An abstract error is an exceptional condition that may arise during the performance of an abstract operation, causing it to fail. When an abstract error is reported, the performer conveys to the invoker the identity of the abstract error and possibly a single information object called its parameter.

Abstract operations and abstract errors are specified as instances of the ABSTRACT-OPERATION and ABSTRACT-ERROR information object classes.

Their definitions are identical to the Remote Operations OPERATION and ERROR information object classes, respectively.

```
ABSTRACT-OPERATION ::= OPERATION

ABSTRACT-ERROR ::= ERROR
```

30 ROS Realization

Once a distributed information processing task has been described and specified in abstract terms, the manner in which each aspect of the task is to be concretely realized must be prescribed. Each aspect may admit of several concrete realizations.

The concrete realization of the components of the MHS abstract service is often trivial when accomplished by means of Remote Operations. This is so because for a given abstract service there exists a ROS-based application protocol that is functionally identical to it. This follows from the fact that the framework for the specification of abstract services is isomorphic to that for the specification of ROS-based application protocols. The correspondences behind the isomorphism are listed in Table 13.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

Table 13 – Correspondence of abstract service components to ROS information object classes

Abstract service component	ROS information object class
MHS-object	ROS-OBJECT-CLASS
Port	OPERATION-PACKAGE
Abstract-operation	OPERATION
Abstract-error	ERROR

The ROS information object classes CONTRACT and CONNECTION-PACKAGE are used directly in the MHS abstract model.

--`,,`-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

Annex A

Directory Object Classes and Attributes

(This annex forms an integral part of this Recommendation | International Standard)

Several Directory object classes, attributes, attribute syntaxes, contexts, and certificate subject alternative names are specific to Message Handling. These are defined in the present annex using the OBJECT-CLASS, ATTRIBUTE, and CONTEXT information object classes of ITU-T Rec. X.501 | ISO/IEC 9594-2, and the OTHER-NAME information object classes of ITU-T Rec. X.509 | ISO/IEC 9594-8, respectively.

A.1 Object Classes

The object classes specific to Message Handling are those specified below.

NOTE – The Directory object classes described in this Annex Can be combined with other object classes, e.g., the ones defined in ITU-T Rec. X.521 | ISO/IEC 9594-7. See also ITU-T Rec. X.501 | ISO/IEC 9594-2, clause 12 for an explanation of how Directory object classes can be combined in one Directory entry. Annex B of ITU-T Rec. X.521 | ISO/IEC 9594-7 gives some further information about Directory name forms and possible Directory Information Tree structures.

A.1.1 MHS Distribution List

An **MHS Distribution List** object is a DL. The attributes in its entry identify its common name, submit permissions, and OR-addresses and, to the extent that the relevant attributes are present, describe the DL, identify its organization, organizational units, and owner; cite related objects; identify its maximum content length, deliverable content types, and acceptable, exclusively acceptable, and unacceptable EITs,; and identify its expansion policy, subscription addresses, archive addresses, related lists and members.

```
mhs-distribution-list OBJECT-CLASS ::= {
       SUBCLASS OF    { top }
       MUST CONTAIN   { commonName |
                        mhs-dl-submit-permissions |
                        mhs-or-addresses }
       MAY CONTAIN    { description |
                        organizationName |
                        organizationalUnitName |
                        owner |
                        seeAlso |
                        mhs-maximum-content-length |
                        mhs-deliverable-content-types |
                        mhs-acceptable-eits |
                        mhs-exclusively-acceptable-eits |
                        mhs-unacceptable-eits |
                        mhs-dl-policy |
                        mhs-dl-subscription-service |
                        mhs-dl-archive-service |
                        mhs-dl-related-lists |
                        mhs-dl-members }
       ID             id-oc-mhs-distribution-list }
```

A.1.2 MHS Message Store

An **MHS Message Store** object is an AE that realizes an MS. The attributes in its entry, to the extent that they are present, describe the MS, identify its owner, and enumerate the attributes, automatic actions, matching rules, content types, and network protocols it supports.

```
mhs-message-store OBJECT-CLASS ::= {
       SUBCLASS OF    { applicationEntity }
       MAY CONTAIN    { owner |
                        mhs-supported-attributes |
                        mhs-supported-automatic-actions |
                        mhs-supported-matching-rules |
                        mhs-supported-content-types |
                        protocolInformation }
       ID             id-oc-mhs-message-store }
```

A.1.3 MHS Message Transfer Agent

An **MHS Message Transfer Agent** object is an AE that implements an MTA. The attributes in its entry, to the extent that they are present, describe the MTA and identify its owner, its maximum content length, and its supported network protocols.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

```
mhs-message-transfer-agent OBJECT-CLASS ::= {
       SUBCLASS OF    { applicationEntity }
       MAY CONTAIN    { owner |
                      mhs-maximum-content-length |
                      protocolInformation }
       ID             id-oc-mhs-message-transfer-agent }
```

A.1.4 MHS User

An **MHS User** object is a generic MHS user. (The generic MHS user can have, for example, a business address, a residential address, or both.) The attributes in its entry identify the user's OR-address and, to the extent that the relevant attributes are present, identify the user's maximum content length, content types, and EITs; its MS; and its preferred delivery methods.

```
mhs-user OBJECT-CLASS ::= {
       SUBCLASS OF    { top }
       KIND           auxiliary
       MUST CONTAIN   { mhs-or-addresses }
       MAY CONTAIN    { mhs-maximum-content-length |
                      mhs-deliverable-content-types |
                      mhs-acceptable-eits |
                      mhs-exclusively-acceptable-eits |
                      mhs-unacceptable-eits |
                      mhs-or-addresses-with-capabilities |
                      mhs-message-store-dn }
       ID             id-oc-mhs-user }
```

If the MHS User has more than one OR-address, which have differing deliverability capabilities, then the attributes mhs-deliverable-content-types, mhs-deliverable-eits, and mhs-undeliverable-eits should represent the union of these deliverability capabilities; the attribute mhs-maximum-content-length should contain the largest of the values of this attribute. The capability of each OR-address can then be determined when required from the attribute mhs-or-addresses-with-capabilities.

NOTE – The MHS User's preferredDeliveryMethod information is inherited in the telecommunicationAttributeSet from the Directory user's naming object class.

A.1.5 MHS User Agent

An **MHS User Agent** object is an AE that realizes a UA. The attributes in its entry, to the extent that they are present, identify the UA's owner; its maximum content length, content types, and EITs; its deliverable classes; its OR-address; and its supported network protocols.

```
mhs-user-agent OBJECT-CLASS ::= {
       SUBCLASS OF    { applicationEntity }
       MAY CONTAIN    { owner |
                      mhs-maximum-content-length |
                      mhs-deliverable-content-types |
                      mhs-acceptable-eits |
                      mhs-exclusively-acceptable-eits |
                      mhs-unacceptable-eits |
                      mhs-deliverable-classes |
                      mhs-or-addresses |
                      protocolInformation }
       ID             id-oc-mhs-user-agent }
```

A.2 Attributes

The attributes specific to Message Handling are those specified below.

A.2.1 MHS Acceptable EITs

The **MHS Acceptable EITs** attribute identifies a set of EITs; the presence of any one of these EITs in a messages makes it a message whose delivery a user will accept, or which a DL will expand, as defined in 8.4.1.1.1.3.1 of ITU-T Rec. X.411 | ISO/IEC 10021-4. The order of precedence between this attribute and those in A.2.10 and A.2.19 is defined in 14.3.4.4 of ITU-T Rec. X.411 | ISO/IEC 10021-4.

A value of this attribute is an Object Identifier.

```
mhs-acceptable-eits ATTRIBUTE ::= {
       WITH SYNTAX                 ExtendedEncodedInformationType
       EQUALITY MATCHING RULE      objectIdentifierMatch
       ID                          id-at-mhs-acceptable-eits }
```


Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

A.2.2 MHS Deliverable Classes

The **MHS Deliverable Classes** attribute identifies the classes of messages whose delivery a UA will accept (see 8.4.1.1.3 in ITU-T Rec. X.411 | ISO/IEC 10021-4).

A value of this attribute is a Capability (see A.3.4).

```
mhs-deliverable-classes ATTRIBUTE ::= {
        WITH SYNTAX                 Capability
        EQUALITY MATCHING RULE      capabilityMatch
        ID                          id-at-mhs-deliverable-classes }
```

A.2.3 MHS Deliverable Content Types

The **MHS Deliverable Content Types** attribute identifies the content types of the messages whose delivery a user will accept, or which a DL will expand. The absence of this attribute indicates that any content type may be delivered (or expanded).

A value of this attribute is an Object Identifier.

```
mhs-deliverable-content-types ATTRIBUTE ::= {
        WITH SYNTAX                 ExtendedContentType
        EQUALITY MATCHING RULE      objectIdentifierMatch
        ID                          id-at-mhs-deliverable-content-types }
```

A.2.4 MHS DL Archive Service

The **MHS DL Archive Service** attribute identifies a service from which a user may request copies of messages previously distributed by this DL. Further specification of any such service (e.g., the format of requests) is beyond the scope of this International Standard.

A value of this attribute is an OR-Name.

```
mhs-dl-archive-service ATTRIBUTE ::= {
        WITH SYNTAX                 ORName
        EQUALITY MATCHING RULE      oRNameExactMatch
        -- EXTENSIBLE MATCHING RULE { oRNameMatch | oRNameElementsMatch |
        --                          oRNameSubstringElementsMatch |
        --                          oRNameSingleElementMatch }--
        ID                          id-at-mhs-dl-archive-service }
```

A.2.5 MHS DL Members

The **MHS DL Members** attribute identifies a DL's members. When a DL is expanded, each of the values of this attribute will become a recipient of the message.

A value of this attribute is an OR-name.

```
mhs-dl-members ATTRIBUTE ::= {
        WITH SYNTAX                 ORName
        EQUALITY MATCHING RULE      oRNameExactMatch
        -- EXTENSIBLE MATCHING RULE { oRNameMatch | oRNameElementsMatch |
        --                          oRNameSubstringElementsMatch |
        --                          oRNameSingleElementMatch }--
        ID                          id-at-mhs-dl-members }
```

A value of this attribute may have an annotation attached to it to provide information for use in the administration of the DL (see A.4.1), or may have an indication attached to it that this member is itself a DL to enable efficient evaluation of DL submit permission (see A.4.2), or may have an indication attached to it that this member uses a non-standard system (see A.4.3).

A.2.6 MHS DL Policy

The **MHS DL Policy** attribute identifies the choice of policy options to be applied when expanding a DL.

A value of this attribute is a DL policy.

```
mhs-dl-policy ATTRIBUTE ::= {
        WITH SYNTAX                 DLPolicy
        SINGLE VALUE                TRUE
        ID                          id-at-mhs-dl-policy }
```


Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

A.2.7 MHS DL Related Lists

The **MHS DL Related Lists** attribute identifies other Distribution Lists which are, in some unspecified way, related to this DL.

A value of this attribute is a Distinguished Name.

```
mhs-dl-related-lists ATTRIBUTE ::= {
        SUBTYPE OF                  distinguishedName
        EQUALITY MATCHING RULE      distinguishedNameMatch
        ID                          id-at-mhs-dl-related-lists }
```

A.2.8 MHS DL Submit Permissions

The **MHS DL Submit Permissions** attribute identifies the users and DLs that may submit messages (or probes) to a DL. It does not affect the handling of reports at DL expansion points.

A value of this attribute is a DL submit permission.

```
mhs-dl-submit-permissions ATTRIBUTE ::= {
        WITH SYNTAX                 DLSubmitPermission
        ID                          id-at-mhs-dl-submit-permissions }
```

A.2.9 MHS DL Subscription Service

The **MHS DL Subscription Service** attribute identifies a service to which a user may request changes to the membership of this DL (e.g., for a user to request to be added to the DL). Further specification of any such service (e.g., the format of requests) is beyond the scope of this International Standard.

A value of this attribute is an OR-Name.

```
mhs-dl-subscription-service ATTRIBUTE ::= {
        WITH SYNTAX                 ORName
        EQUALITY MATCHING RULE      oRNameExactMatch
        -- EXTENSIBLE MATCHING RULE { oRNameMatch | oRNameElementsMatch |
        --                          oRNameSubstringElementsMatch |
        --                          oRNameSingleElementMatch }--
        ID                          id-at-mhs-dl-subscription-service }
```

A.2.10 MHS Exclusively Acceptable EITs

The **MHS Exclusively Acceptable EITs** attribute identifies a set of EITs; the presence of all EITs of a message within this set makes it a messages whose delivery a user will accept, or which a DL will expand, as defined in 8.4.1.1.1.3.1 of ITU-T Rec. X.411 | ISO/IEC 10021-4. The order of precedence between this attribute and those in A.2.1 and A.2.19 is defined in 14.3.4.4 of ITU-T Rec. X.411 | ISO/IEC 10021-4.

NOTE – Implicit conversion may occur in the MTS prior to delivery of a message, so that any EIT originally present in the message but not among the exclusively acceptable EITs may be converted into an exclusively acceptable EIT, thus enabling delivery (or DL expansion).

A value of this attribute is an Object Identifier.

```
mhs-exclusively-acceptable-eits ATTRIBUTE ::= {
        WITH SYNTAX                 ExtendedEncodedInformationType
        EQUALITY MATCHING RULE      objectIdentifierMatch
        ID                          id-at-mhs-exclusively-acceptable-eits }
```

A.2.11 MHS Maximum Content Length

The **MHS Maximum Content Length** attribute identifies the maximum content length of the messages whose delivery a user will accept, or which a DL will expand, or which an MTA will accept.

A value of this attribute is an Integer.

```
mhs-maximum-content-length ATTRIBUTE ::= {
        WITH SYNTAX                 ContentLength
        EQUALITY MATCHING RULE      integerMatch
        SINGLE VALUE                TRUE
        ID                          id-at-mhs-maximum-content-length }
```

A.2.12 MHS Message Store Directory Name

The **MHS Message Store Directory Name** attribute identifies a user's MS by name.

The value of this attribute is a Directory distinguished name.

--`,,`-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

```
mhs-message-store-dn ATTRIBUTE ::= {
       SUBTYPE OF                  distinguishedName
       EQUALITY MATCHING RULE      distinguishedNameMatch
       SINGLE VALUE                TRUE
       ID                          id-at-mhs-message-store-dn }
```

A.2.13 MHS OR-Addresses

The **MHS OR-Addresses** attribute specifies a user's or DL's OR-addresses. The Directory user may choose any one of the values to use as the OR-address of this user.

A value of this attribute is an OR-address.

```
mhs-or-addresses ATTRIBUTE ::= {
       WITH SYNTAX                 ORAddress
       EQUALITY MATCHING RULE      oRAddressMatch
       -- EXTENSIBLE MATCHING RULE { oRAddressElementsMatch |
       --                          oRAddressSubstringElementsMatch |
       --                          oRNameSingleElementMatch } --
       ID                          id-at-mhs-or-addresses }
```

When the MHS OR-Addresses with Capabilities attribute is present in an entry, the MHS OR-Addresses attribute should contain only the user's preferred address.

A.2.14 MHS OR-Addresses with Capabilities

The **MHS OR-Addresses with Capabilities** attribute identifies the deliverability capability of each of a user's OR-addresses.

A value of this attribute is an OR-address with capabilities.

```
mhs-or-addresses-with-capabilities ATTRIBUTE ::= {
       WITH SYNTAX                 AddressCapabilities
       EQUALITY MATCHING RULE      addressCapabilitiesMatch
       ID                          id-at-mhs-or-addresses-with-capabilities }
```

This attribute may be used to indicate the individual capabilities of each of the user's OR-addresses where different addresses have differing capabilities. It may also be used where a single address has, for example, differing capabilities for different content-types. Where there are no differing capabilities which the user requires to distinguish, the MHS OR-Addresses attribute alone is sufficient.

A.2.15 MHS Supported Attributes

The **MHS Supported Attributes** attribute identifies the attributes that an MS fully supports.

A value of this attribute is an Object Identifier.

```
mhs-supported-attributes ATTRIBUTE ::= {
       WITH SYNTAX                 ATTRIBUTE.&id({AttributeTable})
       EQUALITY MATCHING RULE      objectIdentifierMatch
       ID                          id-at-mhs-supported-attributes
         }
```

A.2.16 MHS Supported Automatic Actions

The **MHS Supported Automatic Actions** attribute identifies the automatic actions that an MS fully supports.

A value of this attribute is an Object Identifier.

```
mhs-supported-automatic-actions ATTRIBUTE ::= {
       WITH SYNTAX                 AUTO-ACTION.&id ({AutoActionTable})
       EQUALITY MATCHING RULE      objectIdentifierMatch
       ID                          id-at-mhs-supported-automatic-actions }
```

A.2.17 MHS Supported Content Types

The **MHS Supported Content Types** attribute identifies the content types of the messages whose syntax and semantics an MS fully supports.

A value of this attribute is an Object Identifier.

```
mhs-supported-content-types ATTRIBUTE ::= {
       WITH SYNTAX                 ExtendedContentType
       EQUALITY MATCHING RULE      objectIdentifierMatch
       ID                          id-at-mhs-supported-content-types }
```


Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

A.2.18 MHS Supported Matching Rules

The **MHS Supported Matching Rules** attribute identifies the matching rules an MS fully supports.

A value of this attribute is an Object Identifier.

```
mhs-supported-matching-rules ATTRIBUTE ::= {
       WITH SYNTAX                 MATCHING-RULE.&id ({MatchingRuleTable})
       EQUALITY MATCHING RULE      objectIdentifierMatch
       ID                          id-at-mhs-supported-matching-rules }
```

A.2.19 MHS Unacceptable EITs

The **MHS Unacceptable EITs** attribute identifies a set of EITs; the presence of any one of these EITs in a messages makes it a message whose delivery a user will not accept, or which a DL will not expand, as defined in 8.4.1.1.1.3.1 of ITU-T Rec. X.411 | ISO/IEC 10021-4. The order of precedence between this attribute and those in A.2.1 and A.2.10 is defined in 14.3.4.4 of ITU-T Rec. X.411 | ISO/IEC 10021-4.

NOTE – Implicit conversion may occur in the MTS prior to delivery of a message, so that any EIT originally present in the message but among the unacceptable EITs may be converted into an acceptable EIT, thus enabling delivery (or DL expansion).

A value of this attribute is an Object Identifier.

```
mhs-unacceptable-eits ATTRIBUTE ::= {
       WITH SYNTAX                 ExtendedEncodedInformationType
       EQUALITY MATCHING RULE      objectIdentifierMatch
       ID                          id-at-mhs-unacceptable-eits }
```

A.3 Attribute Syntaxes

The attribute syntaxes specific to Message Handling are those specified below.

A.3.1 DL Submit Permission

The **DL Submit Permission** attribute syntax characterizes an attribute each of whose values is a submit permission.

```
DLSubmitPermission ::= CHOICE {
       individual      [0] ORName,
       member-of-dl    [1] ORName,
       pattern-match   [2] ORNamePattern,
       member-of-group [3] Name}
```

A DL submit permission, depending upon its type, grants submit access to the following zero or more users and DLs:

a) *Individual*: The user or (unexpanded) DL any of whose OR-names is equal to the specified OR-name.

b) *Member-of-dl*: Each member of the DL, any of whose OR-names is equal to the specified OR-name, or of each nested DL, recursively.

c) *Pattern-match:* Each user or (unexpanded) DL any of whose OR-names matches the specified OR-name pattern.

```
ORNamePattern ::= ORName
```

The presence of an emp--ty OR-name pattern (i.e. an ORName containing only an empty BuiltInStandardAttributes Sequence) indicates that any user has submit permission.

```
any-user-may-submit DLSubmitPermission ::=
       pattern-match: { built-in-standard-attributes { } }
```

d) *Member-of-group*: Each member of the group-of-names whose name is specified, or of each nested group-of-names, recursively.

A presented value is equal to a target value of this type if the two are identical, attribute by attribute. Additionally, equality may be declared under other conditions which are a local matter.

A.3.1.1 Procedure for Evaluating DL Submit Permission

When using the MHS DL Submit Permission attribute to determine whether a particular message may be expanded by a DL, the following procedure is applied. If the message contains a DL Expansion History then it is the OR-name of the last DL in the expansion history which is compared with the values of the submit permission attribute, otherwise the OR-name of the originator of the message is compared.

--`,,,`-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

The comparison proceeds against each value of the attribute in turn until the first match occurs whereupon the message has obtained submit permission, or until no more attribute values remain to be compared whereupon the message has failed to obtain submit permission.

NOTE – The Directory does not maintain any ordering of attribute values. Efficiency will usually be achieved by considering *Pattern-match* values, shortest first, followed by *Individual* values.

For each attribute value, the appropriate procedure below is applied:

a) *Individual*

The OR-name from the message is compared with the OR-name from this attribute value using the procedure specified in A.3.1.2.

b) *Member-of-dl*

This attribute value is the OR-name of a DL. The MHS DL Members of that DL are obtained. If any member's OR-name lacks an OR-address component then this is obtained from the MHS OR-Addresses attribute from that member's Directory entry. The OR-name from the message is compared with each member OR-name in turn using the procedure specified in A.3.1.2 until a match occurs.

If no match is found, a Directory look-up is performed on each member OR-name to determine whether it is itself another DL. For each nested DL found, the procedure for *Member-of-dl* is applied, recursively.

c) *Pattern-match*

This attribute value contains elements of an OR-name: that is it may contain some OR-address components, or some RDN components of a Directory Name, or both. If the attribute value is an empty OR-name pattern then submit permission for any user exists.

An OR-name containing no attribute types which are absent from the pattern is constructed by discarding other attributes from the OR-name from the message. This constructed OR-name is compared with the pattern OR-name from this attribute value using the procedure specified in the OR-name-elements-match rule in 12.4.5 of ITU-T Rec. X.413 | ISO/IEC 10021-5.

d) *Member-of-group*

This attribute value is the Directory Name of a Group of Names (see 6.10 in ISO/IEC 9594-7). The Members of that Group of Names are obtained, and an OR-name for each OR-Address of each member is constructed from that member's Directory Name plus that member's MHS OR-Addresses attribute. The OR-name from the message is compared with each member OR-name in turn using the procedure specified in A.3.1.2 until a match occurs.

If no match is found, a Directory look-up is performed on each member's Directory Name to determine whether it is itself another Group of Names. For each nested Group of Names found, the procedure for *Member-of-group* is applied, recursively.

Where a member of a DL or a group has more than one value present in that member's MHS OR-Addresses attribute, then a separate OR-name is constructed for each OR-address.

A.3.1.2 Procedure for Determining Equivalence of OR-Names

The OR-name from the message always contains an OR-address and may also contain a Directory Name. The OR-name from the attribute may comprise either or both a Directory Name and an OR-address; the OR-address will be present if it is present in the attribute value, or if it can be obtained from the Directory for members of DLs or groups.

The OR-names are compared using the OR-name-match rule defined in 12.4.4 of ITU-T Rec. X.413 | ISO/IEC 10021-5.

A.3.2 DL Policy

The DL Policy attribute syntax characterizes an attribute whose value is a DL policy.

--`,,`-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

```
DLPolicy ::= SET {
        report-propagation [0] INTEGER {
                previous-dl-or-originator (0),
                dl-owner (1),
                both-previous-and-owner (2) } DEFAULT previous-dl-or-originator,
        report-from-dl [1] INTEGER {
                whenever-requested (0),
                when-no-propagation (1) } DEFAULT whenever-requested,
        originating-MTA-report [2] INTEGER {
                unchanged (0),
                report (2),
                non-delivery-report (3),
                audited-report (4) } DEFAULT unchanged,
        originator-report [3] INTEGER {
                unchanged (0),
                no-report (1),
                report (2),
                non-delivery-report (3) } DEFAULT unchanged,
        return-of-content [4] ENUMERATED {
                unchanged (0),
                content-return-not-requested (1),
                content-return-requested (2) } DEFAULT unchanged,
        priority [5] INTEGER {
                unchanged (0),
                normal (1),
                non-urgent (2),
                urgent (3) } DEFAULT unchanged,
        disclosure-of-other-recipients [6] ENUMERATED {
                unchanged (0),
                disclosure-of-other-recipients-prohibited (1),
                disclosure-of-other-recipients-allowed (2) } DEFAULT unchanged,
        implicit-conversion-prohibited [7] ENUMERATED {
                unchanged (0),
                implicit-conversion-allowed (1),
                implicit-conversion-prohibited (2) } DEFAULT unchanged,
        conversion-with-loss-prohibited [8] ENUMERATED {
                unchanged (0),
                conversion-with-loss-allowed (1),
                conversion-with-loss-prohibited (2) } DEFAULT unchanged,
        further-dl-expansion-allowed [9] BOOLEAN DEFAULT TRUE,
        originator-requested-alternate-recipient-removed [10] BOOLEAN DEFAULT TRUE,
        proof-of-delivery [11] INTEGER {
                dl-expansion-point (0),
                dl-members (1),
                both (2),
                neither (3) } DEFAULT dl-members,
        requested-delivery-method [12] CHOICE {
                unchanged [0] NULL,
                removed [1] NULL,
                replaced RequestedDeliveryMethod } DEFAULT unchanged:NULL,
        token-encryption-algorithm-preference [13] SEQUENCE OF
                                                    AlgorithmInformation OPTIONAL,
        token-signature-algorithm-preference [14] SEQUENCE OF
                                                    AlgorithmInformation OPTIONAL,
        ... }

AlgorithmInformation ::= SEQUENCE {
        algorithm-identifier             [0] AlgorithmIdentifier,
        originator-certificate-selector  [1] CertificateAssertion OPTIONAL,
        recipient-certificate-selector   [2] CertificateAssertion OPTIONAL}
```

A DL policy may specify values for the following options:

a) *Report propagation*: Whether reports received at the DL expansion point are to be sent to the preceding DL (or the originator if no preceding DL), or to the DL owner, or to both of these;

b) *Report from DL*: Whether the DL expansion point sends a confirmatory delivery report whenever it expands a message which requests one, or whether such reports are sent only either when report propagation is dl-owner or when originator-report is no-report or non-delivery-report;

c) *Originating MTA report*: Whether the MTA report request is unchanged, or set to request both delivery and non-delivery reports, or set to request only non-delivery reports, or set to request audited delivery reports;

d) *Originator report*: Whether the originator's report request is unchanged, or set to request no reports, or set to request both delivery and non-delivery reports, or set to request only non-delivery reports;

e) *Return of content*: Whether the originator's request for return of content is unchanged, or set to request no return, or set to request return with non-delivery reports;

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

f) *Priority*: Whether the originator's setting for priority is unchanged, or set to normal, or set to non-urgent, or set to urgent;

g) *Disclosure of other recipients*: Whether the originator's setting is unchanged, or set to prohibit disclosure, or set to allow disclosure;

h) *Implicit conversion prohibited*: Whether the originator's setting is unchanged, or set to allow implicit conversion, or set to prohibit implicit conversion;

i) *Conversion with loss prohibited*: Whether the originator's setting is unchanged, or set to allow conversion with loss, or set to prohibit conversion with loss;

j) *Further DL expansion allowed*: Whether expansion by any nested DLs is allowed or prohibited;

k) *Removal of originator requested alternate recipient*: Whether the originator's requested alternate recipient setting is unchanged, or removed;

l) *Generation of proof of delivery*: Whether the proof of delivery when requested is generated at the DL expansion point, or by the DL members, or by both, or is not generated;

m) *Requested delivery method*: Whether the originator's setting is unchanged, or removed, or replaced by a specified value;

n) *Token encryption algorithm preference*: Specifies the preference order for asymmetric encryption algorithms to be used to re-encrypt data for each DL member in a token, where the message being expanded contains encrypted data in a token for the DL recipient;

o) *Token signature algorithm preference*: Specifies the preference order for signature algorithms to be used to sign data where this is necessary to create a new token for each DL member, e.g. where the message being expanded contains encrypted data in a token for the DL recipient.

Further details of these policy options are in 14.3.10 in ITU-T Rec. X.411 | ISO/IEC 10021-4.

A.3.3 OR-Address

The syntax of OR-Address is defined in ITU-T Rec. X.411 | ISO/IEC 10021-4 and its semantics in clause 18 of this Specification.

A presented OR-address value is equal to a target OR-address value under the conditions specified in 18.4. Matching rules for OR-address-match, OR-address-elements-match, OR-address-substring-elements-match and OR-name-single-elements-match are defined in 12.4.1, 12.4.2, 12.4.3 and 12.4.7 of ITU-T Rec. X.413 | ISO/IEC 10021-5.

A.3.4 OR-Address with Capabilities

The OR-Address with Capabilities attribute syntax characterizes an attribute whose value identifies the deliverability capability of each of a user's OR-addresses. When an address has to be chosen automatically, the selection between addresses having suitable capabilities will be a local matter. When a human user is making the selection, the description may allow a more appropriate choice to be made.

A value of this attribute is an OR-Address with Capabilities.

```
AddressCapabilities ::= SEQUENCE {
       description GeneralString,
       address ORAddress,
       capabilities SET OF Capability }
Capability ::= SET {
       content-types [0] SET OF ExtendedContentType OPTIONAL,
       maximum-content-length [1] ContentLength OPTIONAL,
       encoded-information-types-constraints [2] EncodedInformationTypesConstraints
                                                                          OPTIONAL,
       security-labels [3] SecurityContext OPTIONAL,
       ... }
```

The address-capabilities-match rule determines whether a presented value is identical with an attribute value of OR-Address with Capabilities. This matching rule is used only for Directory maintenance.

```
addressCapabilitiesMatch MATCHING-RULE ::= {
       SYNTAX   AddressCapabilities
       ID       id-mr-address-capabilities-match }
```

The rule returns *true* if, and only if:

a) the description elements contain equivalent strings;

b) the address elements match following the OR-address-match rule defined in 12.4.1 of ITU-T Rec. X.413 | ISO/IEC 10021-5; and

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

c) the capabilities elements contain equivalent components.

Because of the complexity of the capabilities component, it is not envisaged that the Directory could be expected to be used to determine whether a presented capability requirement could be satisfied by any attribute value. Therefore it is expected that all attribute values will be obtained from the Directory and the assessment performed by the Directory user (e.g., the MTA).

The capability-match rule determines whether a presented value is identical with an attribute value of MHS Deliverable Classes. This matching rule is used only for Directory maintenance.

```
capabilityMatch MATCHING-RULE ::= {
       SYNTAX   Capability
       ID       id-mr-capability-match }
```

The rule returns *true* if, and only if the capabilities contain equivalent components.

A.3.5 OR-Name

The syntax of OR-name is defined in ITU-T Rec. X.411 | ISO/IEC 10021-4 and its semantics in clause 17 of this Specification.

The OR-name-exact-match rule determines whether both the Directory Name and the OR-Address components of an OR-Name match. Each component must match if it is present in either the presented or the target value. A presented OR-name value is equal to a target OR-name value if the OR-address components are equivalent using the rules specified in 18.4, and if the Directory Name components are equivalent using the rules specified in ITU-T Recs. of the X.500-series | ISO/IEC 9594. Additionally, equality may be declared under other conditions which are a local matter.

```
oRNameExactMatch MATCHING-RULE ::= {
       SYNTAX   ORName
       ID       id-mr-orname-exact-match }
```

The rule returns *true* if, and only if:

a) where the presented value contains only an OR-address, the rule matches only an attribute value which does not contain a directory-name and where the OR-address matches following the OR-address-match rule defined in 12.4.1 of ITU-T Rec. X.413 | ISO/IEC 10021-5;

b) where the presented value contains only a directory-name, the rule matches only an attribute value which does not contain an OR-address and where the directory-name matches following the distinguishedNameMatch rule defined in 12.5.2 of ITU-T Rec. X.501 | ISO/IEC 9594-2; and

c) where the presented value contains both an OR-address and a directory-name, the rule matches only an attribute value which contains both and where the OR-address matches following the OR-address-match rule defined in 12.4.1 of ITU-T Rec. X.413 | ISO/IEC 10021-5 and the directory-name matches following the distinguishedNameMatch rule defined in 12.5.2 of ITU-T Rec. X.501 | ISO/IEC 9594-2.

NOTE – The OR-name-exact-match rule does not require identical encoding of the presented and target values.

Matching rules for OR-name-match, OR-name-elements-match, OR-name-substring-elements-match and OR-name-single-elements-match are defined in 12.4.4, 12.4.5, 12.4.6 and 12.4.7 of ITU-T Rec. X.413 | ISO/IEC 10021-5.

A.4 Contexts

The contexts specific to Message Handling are those specified below.

A.4.1 DL Administrator Annotation

The DL Administrator Annotation context associates a value of the MHS DL Members attribute with a textual annotation assigned by, and for the use of, the DL administrator.

```
dl-administrator-annotation CONTEXT ::= {
       WITH SYNTAX CHOICE{
       bmpstring                  BMPString,
       universalstring            UniversalString}
       ID id-con-dl-administrator-annotation
```

A presented value is considered to match a stored value if the presented value is a substring of the stored value.

```
         }
dl-administrator-annotation-use-rule DIT-CONTEXT-USE-RULE ::= {
       ATTRIBUTE TYPE             mhs-dl-members.&id OPTIONAL
       CONTEXTS                   {dl-administrator-annotation} }
```

--`,,`-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

A textual annotation may be associated with each member of the DL, and is used only to enable the DL administrator to associate information with the member to aid the administrator in administering the DL. This may be useful, for example, when an MHS DL Members attribute value omits the Directory Name component and comprises only a numeric OR-address.

A.4.2 DL Nested DL

The DL Nested DL context associates a value of the MHS DL Members attribute with an indication that this member is itself a DL.

```
dl-nested-dl CONTEXT ::= {
       WITH SYNTAX                 NULL
       ID                          id-con-dl-nested-dl }


dl-nested-dl-use-rule DIT-CONTEXT-USE-RULE ::= {
       ATTRIBUTE TYPE              mhs-dl-members.&id OPTIONAL
       CONTEXTS                    {dl-nested-dl} }
```

When this context is associated with an MHS DL Members attribute value, it indicates that the member is itself a (nested) DL. This context may be added by an administrative DUA to facilitate efficient evaluation of the DL Submit Permission option Member-of-DL.

A.4.3 DL Reset Originator

The DL Reset Originator context associates a value of the MHS DL Members attribute with an indication that this member uses, or is reached through, a system which does not send (non-)delivery reports to the last DL identified in the DL Expansion History (as required for conformance to X.400 | ISO/IEC 10021).

```
dl-reset-originator CONTEXT ::= {
       WITH SYNTAX                 NULL
       ID                          id-con-dl-reset-originator }


dl-reset-originator-use-rule DIT-CONTEXT-USE-RULE ::= {
       ATTRIBUTE TYPE              mhs-dl-members.&id
       OPTIONAL CONTEXTS           {dl-reset-originator} }
```

When this context is associated with an MHS DL Members attribute value, if the report propagation element of DL Policy is DL owner (only) then the DL expansion point replaces the originator in the Envelope of the copy of the message for this DL member by the OR-name of the DL owner. This may be useful, for example, when this DL member uses a system conforming to X.400 (1984), or a system using a protocol other than X.400 | ISO/IEC 10021.

A.5 Certificate Subject Alternative Names

The other name forms specific to Message Handling for use in a Certificate's subject alternative name field (see 12.3.2.1 in ITU-T Rec. X.509 | ISO/IEC 9594-8) are those specified below.

A.5.1 MTA Name

The MTA Name alternative name for a Certificate's subject enables a Certification Authority to issue Certificates that contain a certified binding between the MTA Name and the public key.

```
mta-name OTHER-NAME ::= { SEQUENCE {
                                   domain        GlobalDomainIdentifier,
                                   mta-name      MTAName }
       IDENTIFIED BY      id-san-mta-name }
```


Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

Annex B

Reference Definition of Object Identifiers

(This annex forms an integral part of this Recommendation | International Standard)

This annex defines for reference purposes various Object Identifiers cited in the ASN.1 module of Annex C. It uses ASN.1.

All Object Identifiers this Specification assigns are assigned in this annex. The annex is definitive for all but those for ASN.1 modules and MHS itself. The definitive assignments for the former occur in the modules themselves; other references to them appear in IMPORT clauses. The latter is fixed.

```
MHSObjectIdentifiers { joint-iso-itu-t mhs(6) arch(5) modules(0) object-identifiers(0)
              version-1999(1) }
DEFINITIONS IMPLICIT TAGS ::=
BEGIN

-- Prologue

-- Exports everything.

IMPORTS -- nothing --  ;

ID ::= OBJECT IDENTIFIER

-- MHS Aspects

id-mhs-protocols ID ::= {joint-iso-itu-t mhs(6) protocols (0)}
        -- MHS Application Contexts and Protocols
        -- See ITU-T Rec. X.419 | ISO/IEC 10021-6.
id-ipms          ID ::= {joint-iso-itu-t mhs(6) ipms      (1)}
        -- Interpersonal Messaging
        -- See ITU-T Rec. X.420 | ISO/IEC 10021-7.
--  Value {joint-iso-itu-t mhs(6) 2} is no longer defined
id-mts           ID ::= {joint-iso-itu-t mhs(6) mts       (3)}
        -- Message Transfer System
        -- See ITU-T Rec. X.411 | ISO/IEC 10021-4.
id-ms            ID ::= {joint-iso-itu-t mhs(6) ms        (4)}
        -- Message Store
        -- See ITU-T Rec. X.413 | ISO/IEC 10021-5.
id-arch          ID ::= {joint-iso-itu-t mhs(6) arch      (5)}
        -- Overall Architecture
        -- See this Specification.
id-group         ID ::= {joint-iso-itu-t mhs(6) group     (6)}
        -- Reserved.
id-edims         ID ::= {joint-iso-itu-t mhs(6) edims     (7)}
        -- EDI Messaging
        -- See ITU-T Rec. X.435 | ISO/IEC 10021-9.
id-management    ID ::= {joint-iso-itu-t mhs(6) management(9)}
        -- MHS Management
        -- See ITU-T Recs. X.460 — X.467 | ISO/IEC 11588.
id-routing       ID ::= {joint-iso-itu-t mhs(6) routing   (10)}
        -- MHS Routing
        -- See ITU-T Rec. X.412 | ISO/IEC 10021-10.

-- Categories

id-mod ID ::= {id-arch 0} -- modules; not definitive
id-oc  ID ::= {id-arch 1} -- object classes
id-at  ID ::= {id-arch 2} -- attribute types
--  Value {id-arch  3} is no longer defined
id-mr  ID ::= {id-arch 4} -- matching rules
id-con ID ::= {id-arch 5} -- contexts
id-san ID ::= {id-arch 6} -- certificate subject alternative names

-- Modules

id-object-identifiers               ID ::= {id-mod 0} -- not definitive
id-directory-objects-and-attributes ID ::= {id-mod 1} -- not definitive
```


Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

-- Object classes

```
id-oc-mhs-distribution-list      ID ::= {id-oc 0}
id-oc-mhs-message-store          ID ::= {id-oc 1}
id-oc-mhs-message-transfer-agent ID ::= {id-oc 2}
id-oc-mhs-user                   ID ::= {id-oc 3}
id-oc-mhs-user-agent             ID ::= {id-oc 4}
```

-- Attributes

```
id-at-mhs-maximum-content-length                  ID ::= {id-at  0}
id-at-mhs-deliverable-content-types               ID ::= {id-at  1}
id-at-mhs-exclusively-acceptable-eits             ID ::= {id-at  2}
id-at-mhs-dl-members                              ID ::= {id-at  3}
id-at-mhs-dl-submit-permissions                   ID ::= {id-at  4}
id-at-mhs-message-store-dn                        ID ::= {id-at  5}
id-at-mhs-or-addresses                            ID ::= {id-at  6}
-- Value {id-at 7} is no longer defined
id-at-mhs-supported-automatic-actions             ID ::= {id-at  8}
id-at-mhs-supported-content-types                 ID ::= {id-at  9}
id-at-mhs-supported-attributes                    ID ::= {id-at 10}
id-at-mhs-supported-matching-rules                ID ::= {id-at 11}
id-at-mhs-dl-archive-service                      ID ::= {id-at 12}
id-at-mhs-dl-policy                               ID ::= {id-at 13}
id-at-mhs-dl-related-lists                        ID ::= {id-at 14}
id-at-mhs-dl-subscription-service                 ID ::= {id-at 15}
id-at-mhs-or-addresses-with-capabilities          ID ::= {id-at 16}
id-at-mhs-acceptable-eits                         ID ::= {id-at 17}
id-at-mhs-unacceptable-eits                       ID ::= {id-at 18}
id-at-mhs-deliverable-classes                     ID ::= {id-at 19}
id-at-encrypted-mhs-maximum-content-length        ID ::= {id-at  0 2}
id-at-encrypted-mhs-deliverable-content-types     ID ::= {id-at  1 2}
id-at-encrypted-mhs-exclusively-acceptable-eits   ID ::= {id-at  2 2}
id-at-encrypted-mhs-dl-members                    ID ::= {id-at  3 2}
id-at-encrypted-mhs-dl-submit-permissions         ID ::= {id-at  4 2}
id-at-encrypted-mhs-message-store-dn              ID ::= {id-at  5 2}
id-at-encrypted-mhs-or-addresses                  ID ::= {id-at  6 2}
id-at-encrypted-mhs-supported-automatic-actions   ID ::= {id-at  8 2}
id-at-encrypted-mhs-supported-content-types       ID ::= {id-at  9 2}
id-at-encrypted-mhs-supported-attributes          ID ::= {id-at 10 2}
id-at-encrypted-mhs-supported-matching-rules      ID ::= {id-at 11 2}
id-at-encrypted-mhs-dl-archive-service            ID ::= {id-at 12 2}
id-at-encrypted-mhs-dl-policy                     ID ::= {id-at 13 2}
id-at-encrypted-mhs-dl-related-lists              ID ::= {id-at 14 2}
id-at-encrypted-mhs-dl-subscription-service       ID ::= {id-at 15 2}
id-at-encrypted-mhs-or-addresses-with-capabilities ID ::= {id-at 16 2}
id-at-encrypted-mhs-acceptable-eits               ID ::= {id-at 17 2}
id-at-encrypted-mhs-unacceptable-eits             ID ::= {id-at 18 2}
id-at-encrypted-mhs-deliverable-classes           ID ::= {id-at 19 2}
```

-- Matching Rules

```
id-mr-orname-exact-match          ID ::= {id-mr  0}
id-mr-address-capabilities-match  ID ::= {id-mr  1}
id-mr-capability-match            ID ::= {id-mr  2}
```

-- Contexts

```
id-con-dl-administrator-annotation          ID ::= {id-con  0}
id-con-dl-nested-dl                         ID ::= {id-con  1}
id-con-dl-reset-originator                  ID ::= {id-con  2}
```

-- Certificate subject alternative names

```
id-san-mta-name                             ID ::= {id-san  0}
```

```
END -- of MHSObjectIdentifiers
```


Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

Annex C

Reference Definition of Directory Object Classes and Attributes

(This annex forms an integral part of this Recommendation | International Standard)

This annex, a supplement to Annex A, defines for reference purposes the object classes, attributes, and attribute syntaxes specific to Message Handling. It uses the OBJECT-CLASS and ATTRIBUTE information object classes of ITU-T Rec. X.501|ISO/IEC 9594-2.

```
MHSDirectoryObjectsAndAttributes { joint-iso-itu-t mhs(6) arch(5) modules(0) directory(1)
            version-1999(1) }
DEFINITIONS IMPLICIT TAGS ::=
BEGIN
```

-- Prologue

-- Exports everything.

```
IMPORTS
```

-- MHS Object Identifiers

```
id-at-mhs-acceptable-eits, id-at-mhs-deliverable-classes,
id-at-mhs-deliverable-content-types, id-at-mhs-dl-archive-service,
id-at-mhs-dl-members, id-at-mhs-dl-policy, id-at-mhs-dl-related-lists,
id-at-mhs-dl-submit-permissions, id-at-mhs-dl-subscription-service,
id-at-mhs-exclusively-acceptable-eits, id-at-mhs-maximum-content-length,
id-at-mhs-message-store-dn, id-at-mhs-or-addresses,
id-at-mhs-or-addresses-with-capabilities, id-at-mhs-supported-attributes,
id-at-mhs-supported-automatic-actions, id-at-mhs-supported-content-types,
id-at-mhs-supported-matching-rules, id-at-mhs-unacceptable-eits,
id-con-dl-administrator-annotation, id-con-dl-nested-dl, id-con-dl-reset-originator,
id-mr-address-capabilities-match, id-mr-capability-match, id-mr-orname-exact-match,
id-oc-mhs-distribution-list, id-oc-mhs-message-store, id-oc-mhs-message-transfer-agent,
id-oc-mhs-user, id-oc-mhs-user-agent, id-san-mta-name
       ----
       FROM MHSObjectIdentifiers { joint-iso-itu-t mhs(6) arch(5) modules(0)
              object-identifiers(0) version-1999(1) }
```

-- MTS Abstract Service

```
ContentLength, EncodedInformationTypesConstraints, ExtendedContentType,
ExtendedEncodedInformationType, GlobalDomainIdentifier, MTAName, ORAddress, ORName,
RequestedDeliveryMethod, SecurityContext
       ----
       FROM MTSAbstractService { joint-iso-itu-t mhs(6) mts(3) modules(0)
              mts-abstract-service(1) version-1999(1) }
```

-- MS Abstract Service

```
ATTRIBUTE, AUTO-ACTION
       ----
       FROM MSAbstractService { joint-iso-itu-t mhs(6) ms(4) modules(0)
              abstract-service(1) version-1999(1) }
```

-- MS General Attribute Types

```
AttributeTable
       ----
       FROM MSGeneralAttributeTypes { joint-iso-itu-t mhs(6) ms(4) modules(0)
              general-attribute-types(2) version-1999(1) }
```

-- MS General Auto Action Types

```
AutoActionTable
       ----
       FROM MSGeneralAutoActionTypes { joint-iso-itu-t mhs(6) ms(4) modules(0)
              general-auto-action-types(3) version-1994(0) }
```


Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

```
-- MS Matching Rules

        MatchingRuleTable, oRAddressMatch, oRAddressElementsMatch,
        oRAddressSubstringElementsMatch, oRNameMatch, oRNameElementsMatch,
        oRNameSingleElementMatch, oRNameSubstringElementsMatch
                ----
                FROM MSMatchingRules { joint-iso-itu-t mhs(6) ms(4) modules(0)
                        general-matching-rules(5) version-1999(1)}

        -- Information Framework

        ATTRIBUTE, CONTEXT, distinguishedNameMatch, DIT-CONTEXT-USE-RULE,
        objectIdentifierMatch, MATCHING-RULE, Name, OBJECT-CLASS, top
                ----
                FROM InformationFramework {joint-iso-itu-t ds(5) module(1)
                        informationFramework(1) 3 }

        -- Selected Object Classes

        applicationEntity
                ----
                FROM SelectedObjectClasses { joint-iso-itu-t ds(5) module(1)
                        selectedObjectClasses(6) 3 }

        -- Selected Attribute Types

        commonName, description, distinguishedName, integerMatch, organizationName,
        organizationalUnitName, owner, protocolInformation, seeAlso
                ----
                FROM SelectedAttributeTypes { joint-iso-itu-t ds(5) module(1)
                        selectedAttributeTypes(5) 3 }

        -- Authentication Framework

        AlgorithmIdentifier
        ----
        FROM AuthenticationFramework {joint-iso-itu-t ds(5) module(1)
        authenticationFramework(7) 3}

        -- Certificate Extensions

        CertificateAssertion, OTHER-NAME
        ----
        FROM CertificateExtensions {joint-iso-itu-t ds(5) module(1)
        certificateExtensions(26) 0};

-- OBJECT CLASSES

-- MHS Distribution List

mhs-distribution-list OBJECT-CLASS ::= {
        SUBCLASS OF     { top }
        MUST CONTAIN    { commonName |
                          mhs-dl-submit-permissions |
                          mhs-or-addresses }
        MAY CONTAIN     { description |
                          organizationName |
                          organizationalUnitName |
                          owner |
                          seeAlso |
                          mhs-maximum-content-length |
                          mhs-deliverable-content-types |
                          mhs-acceptable-eits |
                          mhs-exclusively-acceptable-eits |
                          mhs-unacceptable-eits |
                          mhs-dl-policy |
                          mhs-dl-subscription-service |
                          mhs-dl-archive-service |
                          mhs-dl-related-lists |
                          mhs-dl-members }
        ID              id-oc-mhs-distribution-list }
```


Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

-- MHS Message Store

```
mhs-message-store OBJECT-CLASS ::= {
       SUBCLASS OF    { applicationEntity }
       MAY CONTAIN    { owner |
                      mhs-supported-attributes |
                      mhs-supported-automatic-actions |
                      mhs-supported-matching-rules |
                      mhs-supported-content-types |
                      protocolInformation }
       ID             id-oc-mhs-message-store }
```

-- MHS Message Transfer Agent

```
mhs-message-transfer-agent OBJECT-CLASS ::= {
       SUBCLASS OF    { applicationEntity }
       MAY CONTAIN    { owner |
                      mhs-maximum-content-length |
                      protocolInformation }
       ID             id-oc-mhs-message-transfer-agent }
```

-- MHS User

```
mhs-user OBJECT-CLASS ::= {
       SUBCLASS OF    { top }
       KIND           auxiliary
       MUST CONTAIN   { mhs-or-addresses }
       MAY CONTAIN    { mhs-maximum-content-length |
                      mhs-deliverable-content-types |
                      mhs-acceptable-eits |
                      mhs-exclusively-acceptable-eits |
                      mhs-unacceptable-eits |
                      mhs-or-addresses-with-capabilities |
                      mhs-message-store-dn }
       ID             id-oc-mhs-user }
```

-- MHS User Agent

```
mhs-user-agent OBJECT-CLASS ::= {
       SUBCLASS OF    { applicationEntity }
       MAY CONTAIN    { owner |
                      mhs-maximum-content-length |
                      mhs-deliverable-content-types |
                      mhs-acceptable-eits |
                      mhs-exclusively-acceptable-eits |
                      mhs-unacceptable-eits |
                      mhs-deliverable-classes |
                      mhs-or-addresses |
                      protocolInformation }
       ID             id-oc-mhs-user-agent }
```

-- ATTRIBUTES

-- MHS Acceptable EITs

```
mhs-acceptable-eits ATTRIBUTE ::= {
       WITH SYNTAX                 ExtendedEncodedInformationType
       EQUALITY MATCHING RULE      objectIdentifierMatch
       ID                          id-at-mhs-acceptable-eits }
```

-- MHS Deliverable Classes

```
mhs-deliverable-classes ATTRIBUTE ::= {
       WITH SYNTAX                 Capability
       EQUALITY MATCHING RULE      capabilityMatch
       ID                          id-at-mhs-deliverable-classes }
```

-- MHS Deliverable Content Types

```
mhs-deliverable-content-types ATTRIBUTE ::= {
       WITH SYNTAX                 ExtendedContentType
       EQUALITY MATCHING RULE      objectIdentifierMatch
       ID                          id-at-mhs-deliverable-content-types }
```

--`,,`-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

-- MHS DL Archive Service

```
mhs-dl-archive-service ATTRIBUTE ::= {
       WITH SYNTAX                 ORName
       EQUALITY MATCHING RULE      oRNameExactMatch
       -- EXTENSIBLE MATCHING RULE { oRNameMatch | oRNameElementsMatch |
       --                          oRNameSubstringElementsMatch | oRNameSingleElementMatch }--
       ID                          id-at-mhs-dl-archive-service }
```

-- MHS DL Members

```
mhs-dl-members ATTRIBUTE ::= {
       WITH SYNTAX                 ORName
       EQUALITY MATCHING RULE      oRNameExactMatch
       -- EXTENSIBLE MATCHING RULE { oRNameMatch | oRNameElementsMatch |
       --                          oRNameSubstringElementsMatch | oRNameSingleElementMatch }--
       ID                          id-at-mhs-dl-members }
```

-- MHS DL Policy

```
mhs-dl-policy ATTRIBUTE ::= {
       WITH SYNTAX                 DLPolicy
       SINGLE VALUE                TRUE
       ID                          id-at-mhs-dl-policy }
```

-- MHS DL Related Lists

```
mhs-dl-related-lists ATTRIBUTE ::= {
       SUBTYPE OF                  distinguishedName
       EQUALITY MATCHING RULE      distinguishedNameMatch
       ID                          id-at-mhs-dl-related-lists }
```

-- MHS DL Submit Permissions

```
mhs-dl-submit-permissions ATTRIBUTE ::= {
       WITH SYNTAX                 DLSubmitPermission
       ID                          id-at-mhs-dl-submit-permissions }
```

-- MHS DL Subscription Service

```
mhs-dl-subscription-service ATTRIBUTE ::= {
       WITH SYNTAX                 ORName
       EQUALITY MATCHING RULE      oRNameExactMatch
       -- EXTENSIBLE MATCHING RULE { oRNameMatch | oRNameElementsMatch |
       --                          oRNameSubstringElementsMatch | oRNameSingleElementMatch }--
       ID                          id-at-mhs-dl-subscription-service }
```

-- MHS Exclusively Acceptable EITs

```
mhs-exclusively-acceptable-eits ATTRIBUTE ::= {
       WITH SYNTAX                 ExtendedEncodedInformationType
       EQUALITY MATCHING RULE      objectIdentifierMatch
       ID                          id-at-mhs-exclusively-acceptable-eits }
```

-- MHS Maximum Content Length

```
mhs-maximum-content-length ATTRIBUTE ::= {
       WITH SYNTAX                 ContentLength
       EQUALITY MATCHING RULE      integerMatch
       SINGLE VALUE                TRUE
       ID                          id-at-mhs-maximum-content-length }
```

-- MHS Message Store Directory Name

```
mhs-message-store-dn ATTRIBUTE ::= {
       SUBTYPE OF                  distinguishedName
       EQUALITY MATCHING RULE      distinguishedNameMatch
       SINGLE VALUE                TRUE
       ID                          id-at-mhs-message-store-dn }
```


Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

-- MHS OR-Addresses

```
mhs-or-addresses ATTRIBUTE ::= {
       WITH SYNTAX                  ORAddress
       EQUALITY MATCHING RULE       oRAddressMatch
       -- EXTENSIBLE MATCHING RULE { oRAddressElementsMatch | oRNameSingleElementMatch |
       --                           oRAddressSubstringElementsMatch } --
       ID                           id-at-mhs-or-addresses }
```

-- MHS OR-Addresses with Capabilities

```
mhs-or-addresses-with-capabilities ATTRIBUTE ::= {
       WITH SYNTAX                  AddressCapabilities
       EQUALITY MATCHING RULE       addressCapabilitiesMatch
       ID                           id-at-mhs-or-addresses-with-capabilities }
```

-- MHS Supported Attributes

```
mhs-supported-attributes ATTRIBUTE ::= {
       WITH SYNTAX                  ATTRIBUTE.&id({AttributeTable})
       EQUALITY MATCHING RULE       objectIdentifierMatch
       ID                           id-at-mhs-supported-attributes
         }
```

-- MHS Supported Automatic Actions

```
mhs-supported-automatic-actions ATTRIBUTE ::= {
       WITH SYNTAX                  AUTO-ACTION.&id ({AutoActionTable})
       EQUALITY MATCHING RULE       objectIdentifierMatch
       ID                           id-at-mhs-supported-automatic-actions }
```

-- MHS Supported Content Types

```
mhs-supported-content-types ATTRIBUTE ::= {
       WITH SYNTAX                  ExtendedContentType
       EQUALITY MATCHING RULE       objectIdentifierMatch
       ID                           id-at-mhs-supported-content-types }
```

-- MHS Supported Matching Rules

```
mhs-supported-matching-rules ATTRIBUTE ::= {
       WITH SYNTAX                  MATCHING-RULE.&id ({MatchingRuleTable})
       EQUALITY MATCHING RULE       objectIdentifierMatch
       ID                           id-at-mhs-supported-matching-rules }
```

-- MHS Unacceptable EITs

```
mhs-unacceptable-eits ATTRIBUTE ::= {
       WITH SYNTAX                  ExtendedEncodedInformationType
       EQUALITY MATCHING RULE       objectIdentifierMatch
       ID                           id-at-mhs-unacceptable-eits }
```

-- ATTRIBUTE SYNTAXES

-- DL Submit Permission

```
DLSubmitPermission ::= CHOICE {
       individual      [0] ORName,
       member-of-dl    [1] ORName,
       pattern-match   [2] ORNamePattern,
       member-of-group [3] Name}

ORNamePattern ::= ORName

any-user-may-submit DLSubmitPermission ::= pattern-match: { built-in-standard-attributes { } }
```


Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

-- DL Policy

```
DLPolicy ::= SET {
       report-propagation [0] INTEGER {
              previous-dl-or-originator (0),
              dl-owner (1),
              both-previous-and-owner (2) } DEFAULT previous-dl-or-originator,
       report-from-dl [1] INTEGER {
              whenever-requested (0),
              when-no-propagation (1) } DEFAULT whenever-requested,
       originating-MTA-report [2] INTEGER {
              unchanged (0),
              report (2),
              non-delivery-report (3),
              audited-report (4) } DEFAULT unchanged,
       originator-report [3] INTEGER {
              unchanged (0),
              no-report (1),
              report (2),
              non-delivery-report (3) } DEFAULT unchanged,
       return-of-content [4] ENUMERATED {
              unchanged (0),
              content-return-not-requested (1),
              content-return-requested (2) } DEFAULT unchanged,
       priority [5] INTEGER {
              unchanged (0),
              normal (1),
              non-urgent (2),
              urgent (3) } DEFAULT unchanged,
       disclosure-of-other-recipients [6] ENUMERATED {
              unchanged (0),
              disclosure-of-other-recipients-prohibited (1),
              disclosure-of-other-recipients-allowed (2) } DEFAULT unchanged,
       implicit-conversion-prohibited [7] ENUMERATED {
              unchanged (0),
              implicit-conversion-allowed (1),
              implicit-conversion-prohibited (2) } DEFAULT unchanged,
       conversion-with-loss-prohibited [8] ENUMERATED {
              unchanged (0),
              conversion-with-loss-allowed (1),
              conversion-with-loss-prohibited (2) } DEFAULT unchanged,
       further-dl-expansion-allowed [9] BOOLEAN DEFAULT TRUE,
       originator-requested-alternate-recipient-removed [10] BOOLEAN DEFAULT TRUE,
       proof-of-delivery [11] INTEGER {
              dl-expansion-point (0),
              dl-members (1),
              both (2),
              neither (3) } DEFAULT dl-members,
       requested-delivery-method [12] CHOICE {
              unchanged [0] NULL,
              removed [1] NULL,
              replaced RequestedDeliveryMethod } DEFAULT unchanged:NULL,
       token-encryption-algorithm-preference [13] SEQUENCE OF AlgorithmInformation OPTIONAL,
       token-signature-algorithm-preference [14] SEQUENCE OF AlgorithmInformation OPTIONAL,
       ... }

AlgorithmInformation ::= SEQUENCE {
       algorithm-identifier             [0] AlgorithmIdentifier,
       originator-certificate-selector  [1] CertificateAssertion OPTIONAL,
       recipient-certificate-selector   [2] CertificateAssertion OPTIONAL}
```

-- OR-Address with Capabilities

```
AddressCapabilities ::= SEQUENCE {
       description GeneralString OPTIONAL,
       address ORAddress,
       capabilities SET OF Capability }

Capability ::= SET {
       content-types [0] SET OF ExtendedContentType OPTIONAL,
       maximum-content-length [1] ContentLength OPTIONAL,
       encoded-information-types-constraints [2] EncodedInformationTypesConstraints OPTIONAL,
       security-labels [3] SecurityContext OPTIONAL,
       ... }
```


Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

```
-- MATCHING RULES

-- OR-Address with Capabilities Match

addressCapabilitiesMatch MATCHING-RULE ::= {
       SYNTAX   AddressCapabilities
       ID       id-mr-address-capabilities-match }

-- Capability Match

capabilityMatch MATCHING-RULE ::= {
       SYNTAX   Capability
       ID       id-mr-capability-match }

-- OR-Name Exact Match

oRNameExactMatch MATCHING-RULE ::= {
       SYNTAX   ORName
       ID       id-mr-orname-exact-match }


-- CONTEXTS

-- DL Administrator Annotation
dl-administrator-annotation CONTEXT ::= {
       WITH SYNTAX CHOICE{
         bmpstring          BMPString,
         universalstring    UniversalString}
       ID id-con-dl-administrator-annotation

         }
dl-administrator-annotation-use-rule DIT-CONTEXT-USE-RULE ::= {
       ATTRIBUTE TYPE              mhs-dl-members.&id OPTIONAL
       CONTEXTS                    {dl-administrator-annotation} }


-- DL Nested DL
dl-nested-dl CONTEXT ::= {
       WITH SYNTAX                 NULL
       ID                          id-con-dl-nested-dl }

dl-nested-dl-use-rule DIT-CONTEXT-USE-RULE ::= {
       ATTRIBUTE TYPE              mhs-dl-members.&id OPTIONAL
       CONTEXTS                    {dl-nested-dl} }


-- DL Reset Originator
dl-reset-originator CONTEXT ::= {
       WITH SYNTAX                 NULL
       ID                          id-con-dl-reset-originator }

dl-reset-originator-use-rule DIT-CONTEXT-USE-RULE ::= {
       ATTRIBUTE TYPE              mhs-dl-members.&id
       OPTIONAL CONTEXTS           {dl-reset-originator} }


-- CERTIFICATE SUBJECT ALTERNATIVE NAMES

-- MTA Name
mta-name OTHER-NAME ::= { SEQUENCE {
                                   domain        GlobalDomainIdentifier,
                                   mta-name      MTAName }
       IDENTIFIED BY      id-san-mta-name }

END -- of MHSDirectory
```


Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex D

Security Threats

(This annex does not form an integral part of this Recommendation | International Standard)

An overview of MHS security threats is provided in 15.1 of ITU-T Rec. X.400 | ISO/IEC 10021-1. This considers threats as they appear in an MHS: access threats, inter-message threats, intra-message threats, and message store threats. These threats can appear in various forms as follows:

a) Masquerade;

b) Message sequencing;

c) Modification of information;

d) Denial of service;

e) Leakage of information;

f) Repudiation;

g) Other MHS threats.

In addition, they may occur by accident or by malicious intent and may be active or passive. Attacks on the MHS will address potential weaknesses and may comprise of a number of threats. This annex deals with individual threats and although consideration is given to a number of broad classes of threat, it is not a complete list.

Table D.1 indicates how these threats can be met using the MHS security services. The list of threats given here is indicative rather than definitive.

D.1 Masquerade

Masquerade occurs when an entity successfully pretends to be a different entity and can take place in a number of ways. An unauthorized MTS-user may impersonate another to gain unauthorized access to MTS facilities or to act to the detriment of the valid user, e.g., to discard his messages. An MTS-user may impersonate another user and so falsely acknowledge receipt of a message by the "valid" recipient. A message may be put into the MTS by a user falsely claiming the identity of another user. An MTS-user, MS, or MTA may masquerade as another MTS-user, MS, or MTA.

Masquerade threats include the following:

a) Impersonation and misuse of the MTS;

b) Falsely acknowledge receipt;

c) Falsely claim to originate a message;

d) Impersonation of an MTA to an MTS-user;

e) Impersonation of an MTA to another MTA.

A masquerade usually consists of other forms of attack and in a secure system may involve authentication sequences from valid users, e.g., in replay or modification of messages.

D.2 Message Sequencing

Message sequencing threats occur when part or all of a message is repeated, time-shifted, or reordered. This can be used to exploit the authentication information in a valid message and resequence or time-shift valid messages. Although it is impossible to prevent replay with the MHS security services, it can be detected and the effects of the threat eliminated.

Message sequencing threats include the following:

a) Replay of messages;

b) Reordering of messages;

c) Pre-play of messages;

d) Delay of messages.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

Table D.1 – Use of MHS Security Services

THREAT	SERVICES
MASQUERADE	
Impersonation and misuse of the MTS	Message Origin Authentication Probe Origin Authentication Secure Access Management
Falsely acknowledge receipt	Proof of Delivery
Falsely claim to originate a message	Message Origin Authentication
Impersonation of an MTA to an MTS-user	Proof of submission Report Origin Authentication Secure Access Management
Impersonation of an MTA to another MTA	Report Origin Authentication Secure Access Management
MESSAGE SEQUENCING	
Replay of messages	Message Sequence Integrity
Re-ordering of messages	Message Sequence Integrity
Pre-play of messages	
Delay of messages	
MODIFICATION OF INFORMATION	
Modification of messages	Connection Integrity Content Integrity
Destruction of messages	Message Sequence Integrity
Corruption of routing and other management information	
DENIAL OF SERVICE	
Denial of communications	
MTA flooding	
MTS flooding	
REPUDIATION	
Denial of origin	Non-repudiation of Origin
Denial of submission	Non-repudiation of Submission
Denial of delivery	Non-repudiation of Delivery
LEAKAGE OF INFORMATION	
Loss of confidentiality	Connection Confidentiality Content Confidentiality
Loss of anonymity	Message Flow Confidentiality
Misappropriation of messages	Secure Access Management
Traffic analysis	Message Flow Confidentiality
OTHER THREATS	
Originator not cleared for Message Security Label	Secure Access Management Message Security Labelling
MTA/MTS-user not cleared for Security Context	Secure Access Management
Misrouting	Secure Access Management Message Security Labelling
Differing labelling policies	

D.3 Modification of Information

Information for an intended recipient, routing information, and other management data may be lost or modified without detection. This could occur to any aspect of the message, e.g., its labelling, content, attributes, recipient, or originator. Corruption of routing or other management information, stored in MTAs or used by them, may cause the MTS to lose messages or otherwise operate incorrectly.

Modification of information threats include the following:

a) Modification of messages;

b) Destruction of messages;

c) Corruption of routing and other management information.

D.4 Denial of Service

Denial of service occurs when an entity fails to perform its function or prevents other entities from performing their functions. This may be a denial of access, a denial of communications (leading to other problems like overload), a deliberate suppression of messages to a particular recipient, or a fabrication of extra traffic. The MTS can be denied if an MTA has been caused to fail or operate incorrectly. In addition, an MTS-user may cause the MTS to deny a service

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

to other users by flooding the service with messages which might overload the switching capability of an MTA or fill up all available message storage space.

Denial of service threats include the following:

a) Denial of communications;

b) MTA failure;

c) MTS flooding.

D.5 Repudiation

Repudiation can occur when an MTS-user or the MTS may later deny submitting, receiving, or originating a message.

Repudiation threats include the following:

a) Denial of origin;

b) Denial of submission;

c) Denial of delivery.

D.6 Leakage of Information

Information may be acquired by an unauthorized party by monitoring transmissions, by unauthorized access to information stored in any MHS entity, or by masquerade. In some cases, the presence of an MTS-user on the system may be sensitive and its anonymity may have to be preserved. An MTS-user other than the intended recipient may obtain a message. This might result from impersonation and misuse of the MTS or through causing an MTA to operate incorrectly. Further details on the information flowing in an MTS may be obtained from observing the traffic.

Leakage of information threats include the following:

a) Loss of confidentiality;

b) Loss of anonymity;

c) Misappropriation of messages;

d) Traffic analysis.

D.7 Other Threats

In a multi- or single-level secure system, a number of threats may exist that relate to security labelling, e.g., routing through a node that cannot be trusted with information of particular value, or where systems use different labelling policies. Threats may exist to the enforcement of a security policy based on logical separation using security labels. An MTS-user may originate a message and assign it a label for which it is not cleared. An MTS-user or MTA may set up or accept an association with a security context for which it does not have clearance.

Other threats include the following:

a) Originator not cleared for message label (inappropriate submit);

b) MTA/MTS-user not cleared for context;

c) Misrouting;

d) Differing labelling policies.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

Annex E

Provision of Security Services in ITU-T Rec. X.411 | ISO/IEC 10021-4

(This annex forms an integral part of this Recommendation | International Standard)

Table E.1 indicates which service elements from ITU-T Rec. X.411 | ISO/IEC 10021-4 may be used to support the security services described in 10.2.

Table E.1 – MHS Security Service Provision

SERVICE	MTS ARGUMENTS/SERVICES
ORIGIN AUTHENTICATION SECURITY SERVICES	
Message Origin Authentication	Message Origin Authentication Check Message Token
Probe Origin Authentication	Probe Origin Authentication Check
Report Origin Authentication	Report Origin Authentication Check
Proof of Submission	Proof of Submission Request Proof of Submission
Proof of Delivery	Proof of Delivery Request Proof of Delivery
SECURE ACCESS MANAGEMENT SECURITY SERVICES	
Peer Entity Authentication	Initiator Credentials Responder Credentials
Security Context	Security Context
DATA CONFIDENTIALITY SECURITY SERVICES	
Connection Confidentiality	Not supported
Content Confidentiality	Content Confidentiality Algorithm Identifier Message Token
Message Flow Confidentiality	Content Type
DATA INTEGRITY SECURITY SERVICES	
Connection Integrity	Not supported
Content Integrity	Content Integrity Check Message Token Message Origin Authentication Check
Message Sequence Integrity	Message Sequence Number Message Token
NON-REPUDIATION SECURITY SERVICES	
Non-Repudiation of Origin	Content Integrity Check Message Token Message Origin Authentication Check
Non-Repudiation of Submission	Proof of Submission Request Proof of Submission
Non-Repudiation of Delivery	Proof of Delivery Request Proof of Delivery
Message Security Labelling	Message Security Label Message Token Message Origin Authentication Check
SECURITY MANAGEMENT SECURITY SERVICES	
Change Credentials	Change Credentials
Register	Register

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex F

Representation of OR-Addresses for Human Usage

(This annex does not form an integral part of this Recommendation | International Standard)

This material is Annex D to Rec. F.401 and is not a part of the ITU-T Recommendation.

F.1 Purpose

An OR-address (specified in clause 18) consists of a set of values of attributes taken from the list shown in Table F.1. In order to represent visually an address to a human user, and to enable the user to enter the address into a user interface, each attribute value needs to be associated with the correct attribute type. Many of the names of attribute types shown in Table F.1 are too long for convenient usage on paper or a screen. There is a need for a format which allows attributes to be represented concisely, e.g., on a business card.

This annex specifies how addresses can be expressed concisely using labels to represent the attribute types. There are three categories of attributes: those standard mnemonic attributes which are most likely to be found in OR-addresses represented for human usage (e.g., on business cards), those used in physical delivery addresses, and other specialised attributes (including domain defined attributes). In order to provide a format which is as concise as possible, many of the labels are single characters. This also makes them less language dependent.

Clause F.3 specifies the format for the representation of addresses, and clause F.4 specifies the characteristics necessary for user interfaces which are intended to be used in conjunction with this format.

F.2 Scope

A labelled format for the communication of OR-addresses to human users is specified. The format consists of a set of pairs of labels and attribute values. The characteristics of a user interface which are necessary to accept addresses given in this format are also specified.

In addition a self-explanatory format is specified which is suitable for use where there is more space, e.g., in printed material and in the user interface.

F.3 Format

F.3.1 General

The objective of the labelled format is to enable OR-addresses to be represented in a format which is concise and which can be accurately transcribed by human users. This can be facilitated by careful consideration of which attributes and values are used to form an OR-address.

If the attributes of an OR-address include characters from an extended character set, human users who do not normally use the same extended character set may have difficulty representing the OR-address or entering it into their messaging system. In this situation, an alias of the OR-address should be provided which is composed entirely of Printable String characters.

NOTE 1 – The policy for structuring OR-addresses needs to be carefully considered. Individual OR-addresses should be allocated within an appropriate division of the address space to reduce to an acceptable level the probability that two users might expect to have the same OR-address. Use of given name or initials is usually sufficient to distinguish between users. It may be inappropriate to reflect too much granularity in organizational-unit-names particularly if the organizational structure is subject to frequent change, or users move between organizational-units.

NOTE 2 – There may be a conflict between the benefits of using long values for attributes which are self explanatory (such as the full name of an organization) and the benefits of shorter values (e.g., to fit concisely on a business card). One solution to this problem is to provide an alternative short attribute value (such as the initials of the organization) as an alias for the long value.

NOTE 3 – If a human user might be uncertain about the existence of a space in an attribute value (particularly when it is typeset), aliases could be provided with and without the space (e.g., "SNOMAIL400" as an alias for "SNOMAIL 400" and "Mac Donald" as an alias for "MacDonald").

NOTE 4 – If an alias is provided for an OR-address, it is desirable that this is implemented in such a way that a consistent (preferred) form of OR-address is generated for all messages originated by the user.

Where national usage permits a single space value for the administration-domain-name in an address, this is represented in the address either by omitting the administration-domain-name attribute, or by showing the administration-domain-name attribute with no value or the value of a space. The value "XX" of country-name may be represented in an address by omitting the country-name attribute.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

F.3.2 Labelled format

F.3.2.1 Syntax

OR-addresses in labelled format consist of delimited pairs of labels and values in the syntax <label> "=" <value>. The labels for each attribute are specified in Tables F.1, F.2 and F.3. (The physical delivery attributes in Table F.2 are included for completeness.) The label and its value are either separated by the character "=", or by the space between two columns in a table. Labels may be represented in upper or lower case, but the use of uppercase is recommended as it is likely to be more visually distinctive.

If label/value pairs appear in sequence on a line, they are separated by delimiters. Delimiters may optionally be followed by one or more spaces. The delimiter character may be either ";" or "/", but only one of these can be used in one OR-address. When the delimiter is "/" the first label is prefixed by "/". The use of a delimiter at the end of a line is optional. If the value of any attribute contains the delimiter character, this should be represented by a pair of delimiter characters.

If an identifier is required to preface a labelled address, it is recommended that "X.400" is used.

If an address is entirely composed of attributes contained in Table F.1, it is recommended that the sequence of attributes in the address is that given in Table F.1. If this sequence is incompatible with normal cultural conventions, an alternative sequence may be adopted for representations of addresses which are primarily intended for use within that culture.

Table F.1 – Standard Attributes of the Mnemonic Address Form

Attribute Type	Definition in subclause	Abbreviation (where necessary)	Label
Given Name	18.3.12	Given name	G
Initials	18.3.12	Initials	I
Surname	18.3.12	Surname	S
Generation Qualifier	18.3.12	Generation	Q
Common Name	18.3.2	Common Name	CN
Organization	18.3.9	Organization	O
Organizational Unit 1	18.3.10	Org.Unit.1	OU1
Organizational Unit 2	18.3.10	Org.Unit.2	OU2
Organizational Unit 3	18.3.10	Org.Unit.3	OU3
Organizational Unit 4	18.3.10	Org.Unit.4	OU4
Private Domain Name	18.3.21	PRMD	P
Administration Domain Name	18.3.1	ADMD	A
Country	18.3.3	Country	C

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Table F.2 – Physical Delivery Attributes

Attribute Type	Definition in subclause	Abbreviation (where necessary)	Label
Physical Delivery Personal Name	18.3.17	PD-person	PD-PN
Extension Postal OR-Address Components	18.3.4	PD-ext.address	PD-EA
Extension Physical Delivery Address Components	18.3.5	PD-ext.delivery	PD-ED
Physical Delivery Office Number	18.3.15	PD-office number	PD-OFN
Physical Delivery Office Name	18.3.14	PD-office	PD-OF
Physical Delivery Organization Name	18.3.16	PD-organization	PD-O
Street Address	18.3.22	PD-street	PD-S
Unformatted Postal Address	18.3.25	PD-address	PD-A1
			PD-A2
(there are individual labels for			PD-A3
each line of the address)			PD-A4
			PD-A5
			PD-A6
Unique Postal Name	18.3.26	PD-unique	PD-U
Local Postal Attributes	18.3.6	PD-local	PD-L
Postal Restante Address	18.3.20	PD-restante	PD-R
Post Office Box Address	18.3.18	PD-box	PD-B
Postal Code	18.3.19	PD-code	PD-PC
Physical Delivery Service Name	18.3.11	PD-service	PD-SN
Physical Delivery Country Name	18.3.13	PD-country	PD-C

Table F.3 – Other Attributes

Attribute Type	Definition in subclause	Abbreviation (where necessary)	Label
X.121 Network Address	18.3.7	X.121	X.121
E.164 Network Address	18.3.7	ISDN	ISDN
PSAP Network Address	18.3.7	PSAP	PSAP
Numeric User Identifier	18.3.8	N-ID	N-ID
Terminal Identifier	18.3.23	T-ID	T-ID
Terminal Type	18.3.24	T-TY	T-TY
Domain Defined Attribute	18.1	DDA:<type>	DDA:<type>

where the notation <type> identifies the type of domain defined attribute.

EXAMPLE

X.400: G=john; S=smith; O=a bank ltd; P=abl; A=snomail; C=aq

The address above may also be laid out as a table:

G	John
S	Smith
O	A Bank Ltd
P	ABL
A	Snomail
C	AQ

F.3.2.2 Terminal-type

There are currently six terminal-types defined in 18.3.24, and if international consistency is required the following specific abbreviations should be used to represent the values for these types: tlx, ttx, g3fax, g4fax, ia5 and vtx.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

F.3.2.3 Domain-defined Attribute

The label for a domain-defined attribute consists of "DDA:" followed by the domain-defined attribute type. If an address includes more than one domain-defined attribute of the same type, it is assumed that the domain-defined attributes are intended to be processed in the sequence in which they are represented.

EXAMPLE

DDA:RFC-822=fred(a)widget.co.uk; O=gateway; P=abc; C=gb

If the type of a domain-defined attribute includes the character "=", it is represented by "\=". If the type of a domain-defined attribute includes the character "\", it is represented by "\\". No special representation is required if the type of a domain-defined attribute includes the delimiter character ";" or "/".

F.3.3 Self-explanatory format

The self-explanatory format may be used when space is available. It consists of a list of the attribute types, either in full or abbreviated. The attribute types or abbreviations may be in any language, but each attribute type or abbreviation is followed by the label specified in Table F.1, F.2, or F.3. If English language abbreviations are used, they should be those given in Tables F.1, F.2 and F.3.

If an address is entirely composed of attributes contained in Table F.1, it is recommended that the sequence of attributes in the address is that given in Table F.1. If this sequence is incompatible with normal cultural conventions, an alternative sequence may be adopted for representations of addresses which are primarily intended for use within that culture.

EXAMPLE 1 – Using attribute types in the Norwegian language

Fornavn (G)	Per
Etternavn (S)	Hansen
Organisasjon (O)	Teledir
Organisasjonsenhet (OU1)	Forskning
Privat domene (P)	Tele
Administrasjonsdomene (A)	Telemax
Land (C) NO	

EXAMPLE 2 – Using attribute types and abbreviations in the English language

Given name (G)	John
Surname (S)	Smith
Organisation (O)	A Bank Ltd
Org. Unit (OU1)	IT Dept
Org. Unit (OU2)	MSG Group
PRMD (P)	ABL
ADMD (A)	Snomail
Country (C)	AQ

F.4 User Interface

This clause specifies the characteristics of a user interface which are necessary to enable a user to input OR-addresses represented in either of the formats specified in clause F.3.

It is necessary for the user interface to be able to accept any valid combination of attributes from Tables F.1, F.2 and F.3 which are entered.

If the user interface lists the attributes given in Table F.1, it is recommended to use either the sequence in Table F.1 or, if this sequence is incompatible with normal cultural conventions, the alternative sequence adopted within a particular culture.

If the user supplies a value for the private-domain-name attribute but omits the administration-domain-name attribute, or omits the value for the administration-domain-name attribute, the administration-domain-name value to be used is a single space.

If the user supplies a value for the private-domain-name attribute or the administration-domain-name attribute but omits the country-name attribute, the country-name value to be used is "XX".

Where an OR-address is input as a single string (e.g., in a command line interface), it is necessary to accept any valid labelled format address allowing the user to enter either delimiter. The interface should not require the attributes to be specified in any particular order. The interface should accept labels in upper or lower case.

NOTE – For some existing command line interfaces it may be necessary to enclose the whole labelled format address in quotes.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

If any other type of interface is provided (e.g., a prompting or form-fill interface), it is necessary to provide a means which enables the user to associate easily the identity of each attribute with the labels specified in Tables F.1, F.2 and F.3.

NOTE 1 – One way to associate the identity of each attribute with the labels is to follow the attribute type (or abbreviation) for each attribute with the label in brackets, for example:

Given name (G)
Initials (I)
Surname (S)
Generation Qualifier (Q)
Common Name (CN)
Organisation (O)
Organisational Unit 1 (OU1)
Organisational Unit 2 (OU2)
Organisational Unit 3 (OU3)
Organisational Unit 4 (OU4)
Private Management Domain Name (P)
Administration Management Domain Name (A)
Country (C)

NOTE 2 – Many users may have difficulty copying an address presented as a table (either in labelled or self-explanatory format) into a command line interface which uses delimiters.

NOTE 3 – For form-fill style interfaces, user performance will be optimised when the interface most closely resembles the format of the supplied address with the same sequence of attributes using the same attribute types or labels.

EXAMPLES OF APPLICATION

1 – The Norwegian user of a command line interface receives a business card containing the following OR-address:

G=john; S=smith; O=a bank ltd; P=abl; A=snomail; C=aq

The command line interface enables the user to type in the address exactly as presented on the card.

2 – The Norwegian user of a form fill interface receives the same business card. The form on the screen includes the following field names:

Fornavn (G)
Etternavn (S)
Organisasjon (O)
Privat domene (P)
Administrasjonsdomene (A)
Land (C)

The user is able to fill in the form by associating the single letter labels on the business card with the same labels in brackets after the Norwegian names of the attributes on the screen. (For form fill input the delimiters are not used.)

3 – The English speaking user of a command line interface receives a document quoting the following OR-address:

Fornavn (G)	Per
Etternavn (S)	Hansen
Organisasjon (O)	Teledir
Organisasjonsenhet (OU1)	Forskning
Privat domene (P)	Tele
Administrasjonsdomene (A)	Telemax
Land (C)	NO

The user knows how to transform the address from self-explanatory to labelled format. The user can choose to enter the address with either delimiter, e.g.:

g=per;s=hansen;o=teledir;ou1=forskning;p=tele;a=telemax;c=no

or:

/g=per/s=hansen/o=teledir/ou1=forskning/p=tele/a=telemax/c=no

]

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

Annex G

Use of OR-Addresses by Multinational Organizations

(This annex does not form an integral part of this Recommendation | International Standard)

See also Annex E of ITU-T Rec. F.400.

It is recognised that, where regulations permit, many organizations will wish to operate message handling systems which are located in more than one country. These organizations include both private organizations and public MH service providers. The addressing and routing policies of such systems should be consistent with the general MHS model, in order to ensure interworking with the remainder of the global MHS.

The availability of directory services may significantly affect the addressing policies which organizations choose to adopt. If a universal directory service is available, originators and recipients of messages can be referred to by means of a user-friendly directory name; the OR-addresses can be obtained from the directory by the message handling system. In this situation, the human users need never encounter the OR-address values used, and the addressing policy can be chosen on purely technical criteria. If such a directory service is not available, it will be necessary for users to handle OR-addresses manually. In this case, aesthetic and other human factors considerations will also influence the selection of addressing policy.

G.1 Addressing principles

Global unambiguousness of MHS names is achieved by means of a hierarchical registration structure and consistent use of the naming conventions. This means that wherever an OR-address is used, it is necessary to register the address attribute values according to the procedures applicable for the country denoted by the value of the country-name attribute. In the case of the private-domain-name and administration-domain-name, this implies registration with the applicable registration authorities in that country or domain. These principles form the basis for global messaging.

The interconnection of domains (PRMD to ADMD, ADMD to ADMD, PRMD to PRMD) is subject to bilateral agreement. Such agreements are subject to commercial and technical criteria; among other matters, these agreements may specify the range of OR-address values which are accepted.

Where an organization requires domain names with more than one country code, it is necessary to register the names according to the procedures in each country. Frequently, it will be possible to register the same value of private-domain-name (or administration-domain-name, as applicable) in each country; however, factors outside the scope of MHS (such as legal ownership of names) mean that it will sometimes be necessary for a multinational organization to use different values for their domain name according to the country-code used.

Users of MHS ideally would like to have one address to be used for global messaging which will be provided on letter heads and business cards (indicating the country in which the user is located) to be used by potential partners for communication through MHS systems. The reachability of distant partners through a service provider depends upon the connectivity offered.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

G.2 Example configurations

Multinational organizations may choose to organise their messaging systems in any way which is compatible with these basic principles. Examples of possible configurations for a Multinational PRMD include:

G.2.1 Multiple Independent PRMDs

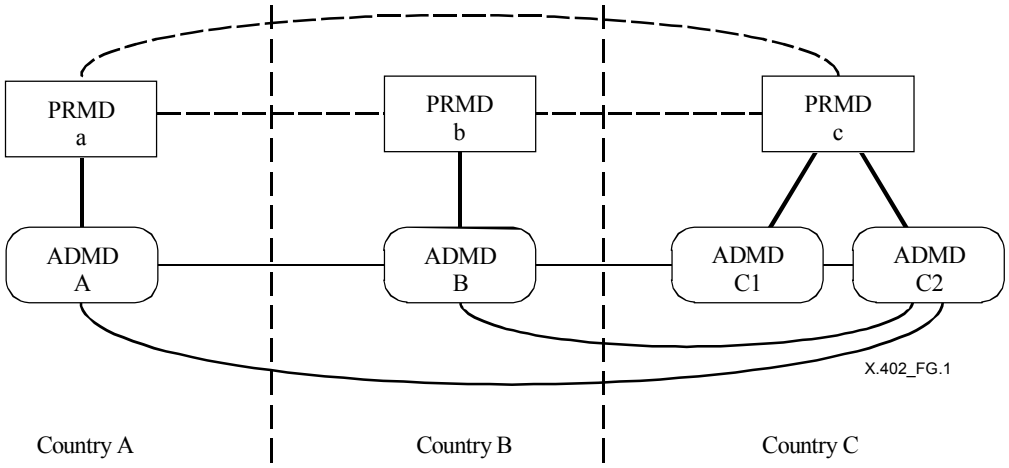


Figure G.1 – Multinational Organizations Multiples: Independent PRMDs

The multinational organization may divide its messaging system logically into portions which are wholly contained within one country. Each portion functions as a separate PRMD, and uses addresses registered in the local country.

Each PRMD may connect to one or more ADMDs in the local country. Where the PRMD is connected to more than one ADMD, and the single space ADMD name is not used, each user (or DL) will have multiple OR-addresses (aliases) with different values for the administration-domain-name attribute. Any of these alias values may be used as the value of the originator OR-address. Where the local country permits the use of the single space ADMD name, and the PRMD elects to use it, each user (or DL) may have a single value of OR-address, regardless of the number of ADMDs that the PRMD is connected to, assuming that mechanisms are in place to handle this convention.

NOTE 1 – The choice of alias name has a number of consequences, see G.3.

NOTE 2 – MTS procedures may need to be revised to support multinational PRMDs in a global messaging environment.

This case is not specific to multinational organizations: it is indistinguishable from multiple PRMDs operated by separate organizations.

This configuration allows for differing regulations in various countries and still provides for the allocation of unique OR-addresses.

G.2.2 A single PRMD, named from a "home" country

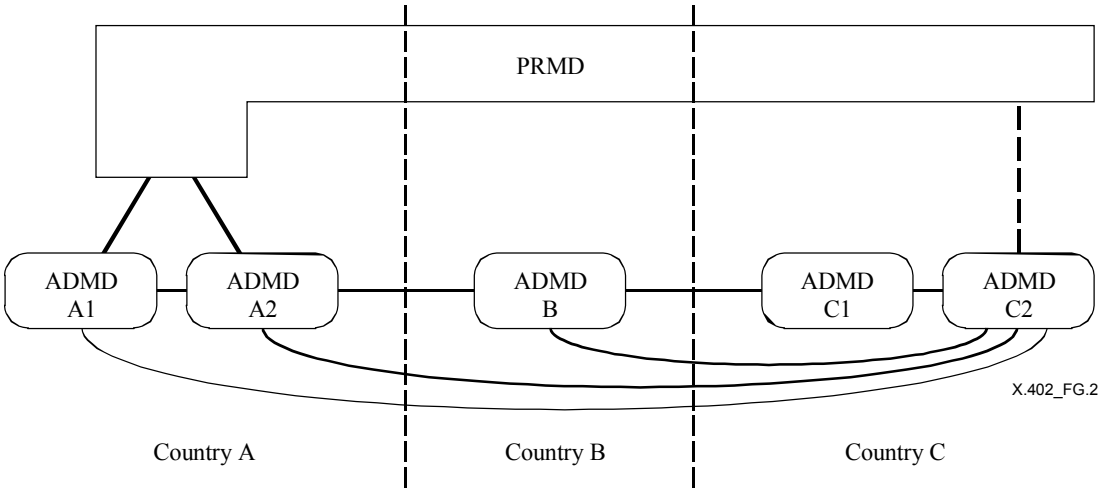


Figure G.2 – A single PRMD with a single name

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

The multinational organization may operate a single management domain which is physically located in more than one country. A single country is selected as the home country for addressing purposes. In this case, all UAs within the MD are addressed with the same values for country-name, administration-domain-name and private-domain-name. This set of attribute values is registered according to the requirements of the chosen country.

The PRMD may connect to one or more ADMDs in the home country, and also (subject to national regulation and commercial criteria) to ADMDs in other countries. Connection to ADMDs outside the home country requires that those ADMDs are able and willing to route messages directly to a PRMD when the country-name used in the OR-address is different from that used by the ADMD.

Users of such a PRMD may not be satisfied with the resulting use of a country name in the OR-address that they may not belong to.

NOTE – MTS procedures may need to be revised to support multinational PRMDs in a global messaging environment.

G.2.3 A single PRMD with multiple country and domain names

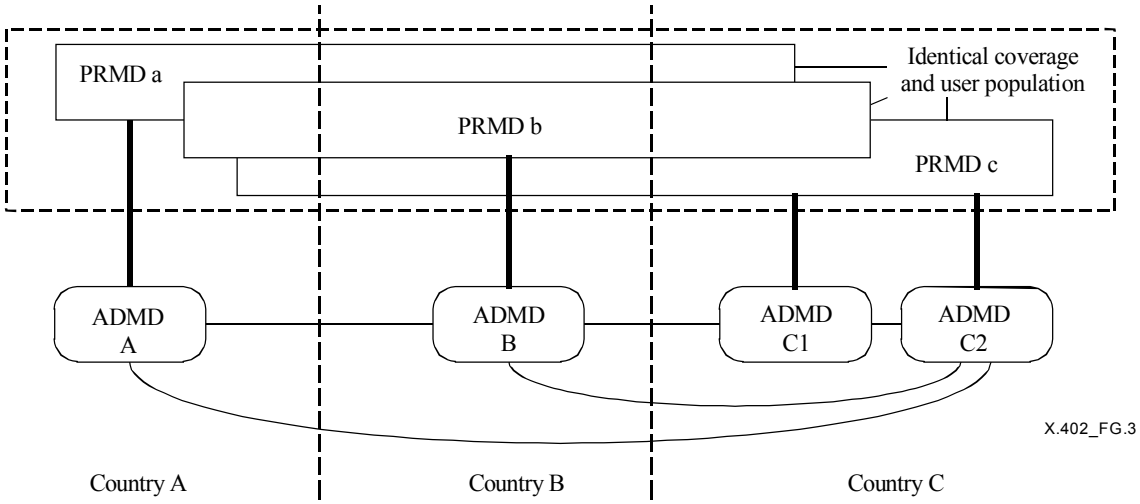


Figure G.3 – A single PRMD with multiple country and domain names

The multinational organization may operate a single messaging system, but use PRMD names registered in more than one country. When forming OR-addresses, the administration-domain-name should be one of the values permitted by the country denoted by the value of the country-name. The private-domain-name value used in a particular OR-address should be one which is registered in a way which is compatible with the country name and administration-domain name, following the procedures of the country or ADMD concerned.

The multinational PRMD may connect to one or more ADMDs. Each user (or DL) now has multiple alias OR-addresses, with different values for the country-name, administration-domain-name and private-domain-name. Any of these may be used as the value of the originator OR-address; users may choose to use an address which identifies the country where they are physically located, but there is no compulsion to do so, provided that the ADMD concerned accepts the originator's OR-address.

If multiple OR-addresses (aliases) appear for the same user, the partners of this user may have problems coping with the situation. The sender and recipient need to understand which of the various OR-addresses should be used at different instances. Lack of understanding will hinder useful open communication. Furthermore, the charges for a certain message may vary depending on the access point chosen for the first ADMD.

NOTE 1 – The choice of alias name has a number of consequences, see G.3.

The bilateral agreements between the PRMD and each ADMD to which it connects will identify the criteria used by the ADMD to route messages into the PRMD. Such agreements may choose to route directly messages addressed to any of the aliases identifying the PRMD, or may route directly only those messages addressed using the local country code, routing others via an ADMD in the country specified in the recipient OR-address, as long as charging and accounting principles can be applied by service providers involved.

NOTE 2 – MTS procedures may need to be revised to support multinational PRMDs in a global messaging environment.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

G.3 Alias OR-addresses

The cases outlined above show that alias management domain names can arise. The presence of alias has a number of implications, both for users and for system implementors.

NOTE – Alias addresses may also occur for users within a domain; treatment of these is usually independent of management domain aliases.

An individual user may select a preferred ADMD from those available, and quote the corresponding country-name, administration-domain-name and private-domain-name when communicating his OR-address, such as on a business card or in the originator OR-address of messages.

If the user also wishes to use the services of other ADMDs to which the PRMD is connected, some difficulties may arise. In certain restricted circumstances, it may be possible for the user (or user agent) to select another combination of ADMD name and PRMD name corresponding to the ADMD which is now to be used, and change the originator OR-address accordingly. However, this is only possible in the case where all the recipients of a message are reached via the same ADMD, and the choice of ADMD is known at the time of submission. It is not possible to change the OR-address after submission, as this conflicts with security services. Also, users may become confused if they receive messages from the same originator but with different OR-addresses.

For these reasons, it may be more satisfactory for the user to use only one OR-address, and for some ADMDs to accept messages where the originator OR-address does not correspond to that country-name and administration-domain-name. Originator OR-addresses which may not correspond to the local PRMD will also arise if the facilities of distribution lists and redirections (e.g., the recipient-assigned-alternate-recipient facility) are implemented. Bilateral agreements between the ADMD operators have to take account of the use of these possibilities (amongst others) in the case of transit via more than one domain. Global reachability is achievable, at least in principle.

The originator OR-address used when sending messages may affect the route taken by messages which may be sent in reply. In the general case, reply messages will be routed via the country and ADMD specified in the OR-address. Bilateral agreements between PRMDs or between the PRMD and ADMDs may allow other routes to be used. These factors will influence the user in selecting an appropriate domain name for use in the OR-address. It should be born in mind that multiple OR-addresses for the same user also have impact on the potential recipients. This confusing situation may not promote useful open communication.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

Annex H

Use of Protected Passwords for Message Store Access

(This annex does not form an integral part of this Recommendation | International Standard)

The purpose of the protected password mechanism in MS-Bind is to allow users to authenticate themselves to a Message Store when using an insecure network, without the risk that the password used can be obtained by someone monitoring traffic on the network. This problem arises in LAN environments (such as Ethernet), where any station connected to the network can inspect all of the traffic passing across the network. Similarly, the administrators of public wide-area networks may not be trusted.

The obvious solution is to encrypt all of the traffic passing over untrusted networks, but additional processing time or administration required by such a system may not be considered cost-effective. Also, use of strong encryption is legally restricted in many areas. The protected password mechanism can be implemented at minimal cost, and by using hashing algorithms rather than full encryption avoids most of the legal issues. While the data is still unprotected, the potential risk is limited to the amount of data retrieved from the MS during a session, whereas obtaining the password would allow an intruder to access the entire content of the MS and also to mount denial-of-service or masquerade attacks. Protected password is therefore a useful compromise, offering a worthwhile increase in security for little cost.

The basis of the Protected Password scheme is the use of cryptographic hash algorithms. These are mathematical algorithms which produce an output related to their input data, but with the property that it is computationally infeasible to determine which input value produces a given output, nor to determine any other input value which would produce the same output.

The simplest possible protected password algorithm would be to take the password typed by the user, pass it through a hash algorithm and transmit the result. The intruder would only be able to see the hashed value, and would not be able to work out the original password. Unfortunately, this does not provide much extra security, because the intruder does not need to know the clear-text of the password: since the password will always hash to the same value, the intruder merely needs to construct a UA that can re-play the recorded value of the hashed password and the MS will accept it.

The solution to this problem is to add a random number to the password before computing the hash value. The UA then sends the hashed password to the MS, accompanied by the chosen value of random number. The MS will know the real password, and can perform the same calculation using the random value supplied by the UA: if the hash calculation gives the same result as that supplied by the UA, then the user must have typed the correct password. This can be represented mathematically as:

Definition: `protected = F (password + random)`
UA sends to MS: `protected, random)`
MS stores: `protected, all used values of random)`

The intruder can obtain the value of `protected` and also the value of `random` used, but still cannot work out the original value of `password`. Furthermore, if the MS keeps track of all values of `random` that have been used in the past and does not allow the same value to be used again, the intruder cannot even gain access by re-sending the same data as had been observed to work in the past.

As it is rather inconvenient for the MS to keep a list of all the `random` values that have been used in the past (there may be a large number of these), it is preferable to use the current date and time in place of (or in addition to) the random number. The MS simply records the most recent time to have been used, and requires that each new connection attempt should use a later time than the time recorded[1)]. This again ensures that every connection will use a new value of protected and prevents the intruder from gaining access. This version becomes:

Definition: `protected = F (password + random + time)`
UA sends to MS: `protected, random, time)`
MS stores: `password,` last value of `time)`

---

1) The MS may also validate that the time is approximately correct for the current real world time-of-day. This is not required for the purposes of authentication, but prevents a user being locked out by inadvertently using a machine whose clock is seriously fast or slow.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

This version provides good protection against external attack, but has the disadvantage that the MS must store the in-clear version of the user's password. This is considered undesirable, as the passwords may be disclosed inadvertently during system maintenance, and because it is extremely easy for a corrupt system administrator to disclose the passwords. The Protected Password scheme specified for MHS adds an extra layer of hashing so that the MS no longer stores the in-clear passwords[2)]:

Definition: `protected1 = F1 (password + random1 + time1)`
Definition: `protected2 = F2 (protected1 + time2 + random2)`
UA stores: `time1, random1`
UA sends to MS: `protected2, time2,` and/or `random2,` optionally `time1` and/or `random1`
MS stores: `protected1,` last used `time2` optionally `time1`, `random1`

In this scheme, the UA first computes `protected1` using a known (pre-configured) value of `time1` and `random1` plus the user's password. It then chooses `random2` and reads the clock for `time2` and computes `protected2`. The data sent to the MS includes at least `protected2`, `time2` and `random2`. The MS then takes the stored value of `protected1` plus the supplied `time2` and `random2` to compute another version of `protected2` – if this agrees with the UA's `protected2`, the user is authenticated.

The protocol allows a wide choice of algorithms, allowing different algorithms for `F1()` and `F2()` and allowing any of `time1`, `time2`, `random1`, `random2` to be omitted. The exact use of the time and random parameters will depend on the algorithms used and the security policy. However, it will normally be necessary to use at least one of `time2`/`random2` to ensure that the hash value is different every time; the MS must store enough information about previous values of `time2`/`random2` to prevent the same combination from being used again in the future (the time is particularly convenient for this). The basic password protection only makes use of time1/`random1` to ensure that two users who have chosen the same password have different values of `protected1` (this makes 'dictionary' attacks less effective); however security policies may use these fields for additional purposes such as password ageing/expiry or to select between multiple different passwords.

The range of possibilities can be illustrated by three examples:

- If in-clear passwords at the MS are acceptable, `F1()` can be made a null function (one which returns its input unchanged) and `time1`, `random1` can be omitted – giving a single level of hashing. `random1` can also be omitted.
- A typical implementation might use the same hash function for both `F1()` and `F2()` and ignore `random2` and `time1`, transmitting only `protected` and `time2` in the bind argument and taking `random1` from configuration.
- A more complex implementation might require the MS to store more than one password (i.e. `protected1` value) for each user, and so would transmit the `time1`/`random1` values to indicate which one the UA is using.

The MS does not need to store `time1`/`random1` if protected passwords are used for every connection. However, the Protected Password scheme can inter-operate with the normal Simple Password authentication if the MS also stores `time1`/`random1`. In the case where a UA has supplied a Simple Password to an MS which is designed for Protected Password, the MS simply computes a value of `protected1` from the supplied password and the stored `time1`, `random1` and compares the result with the stored `protected1`. Similarly, if the user changes the password with the standard change-credentials, the MS can compute a new `protected1` from the supplied new password and the stored `time1`/`random1`.

Providing a protected mechanism to change the password is more difficult. It is of no use to supply the new password in the form of a `protected2` value, as the MS needs to store `protected1` and it is fundamental to the whole scheme that `protected1` cannot be computed from `protected2`. Nor can the new `protected1` be sent directly, since exposing the new `protected1` to an intruder is almost as bad as disclosing the clear password. However, the MS and the UA do have a shared secret in the form of the old value of `protected1`. The new `protected1` can be expressed as a change which must be applied to the old `protected1` to yield the new `protected1`. Since only the change information is transmitted, an intruder who did not know the old `protected1` will still not know the new `protected1`. If the hash

---

2) It should be noted that while the protection against external attack is quite strong, the protection against internal attack (i.e. system administrators reading the files where the MS stores the passwords) is more cosmetic in nature. While the passwords are no longer stored in-clear, the stored protected1 is all that is theoretically needed to gain access to the MS, given a suitably adapted UA. However, an intruder who can read the MS's password file can most probably read the mailbox files too, so the protection merely needs to guard against inadvertent disclosure rather than deliberate attack.

--`,,`-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

algorithm `F1()` has the characteristic that it produces a fixed-size result (as most such algorithms do), then the change can be specified as a bit-string to be exclusive-ORed with the old `protected1` to give the new `protected1`. The number of bits changing does not give the intruder any useful information, since a good hash algorithm will have the characteristic that a small change in the input may give rise to a large change in the output. For hash algorithms with variable-length output, a more complex change description will be required, but the same principles apply.

--`,,`-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex I

Differences Between ISO/IEC 10021-2 and ITU-T Rec. X.402

(This annex does not form an integral part of this Recommendation | International Standard)

This annex identifies the technical differences between ITU-T Rec. X.402 and ISO/IEC 10021-2.

The following are the differences that exist:

a) The ITU-T Recommendation suggests that the direct interconnection of PRMDs may be "impacted by regulation" while the ISO/IEC Standard does not. (See Figure 11.)

b) In both this ISO/IEC Standard and the corresponding ITU-T Recommendation OR-addresses are hierarchically structured, but the ITU-T Recommendation gives responsibility for administration of this hierarchy to ADMDs whereas the ISO/IEC Standard allows the hierarchy to be managed independently (e.g., by national registration authorities). (See clauses 14.1.1, 14.1.2, and 15.)

   The ITU-T Recommendation requires that inter-domain routing follows this hierarchy (so that all routing of messages between PRMDs necessarily involves the services of one or more ADMDs), whereas the ISO/IEC Standard permits the direct connection of PRMDs (e.g., by bilateral agreement) in addition. (See clause 19.)

c) In 18.3.1, the paragraph defining the single space administration-domain-name is a normative part of the ISO/IEC Standard but it is a Note in the ITU-T Recommendation. The paragraph defining the single zero administration-domain-name is a normative part of the ISO/IEC Standard but is omitted from the ITU-T Recommendation.

d) The Representation of OR-Addresses for Human Usage (Annex F) is an informative annex to the ISO/IEC Standard but is informative Annex B of ITU-T Rec. F.401 and not part of ITU-T Rec. X.402.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

Annex J

Summary of Changes to Previous Editions

(This annex does not form an integral part of this Recommendation | International Standard)

J.1 Differences between ISO/IEC 10021-2:1990 and CCITT Rec. X.402 (1992)

The technical differences are as follows:

a) The addition of Annex G on Use of OR-Addresses by Multinational Organizations;

b) The use of additional standard attributes in terminal OR-addresses.

J.2 Differences between CCITT Rec. X.402 (1992) and ITU-T Rec. X.402 (1995) | ISO/IEC 10021-2:1996

The technical differences are as follows:

a) The addition of Annex F on Representation of OR-Addresses for Human Usage;

b) Nine new Directory Attribute definitions (see A.2.1, A.2.2, A.2.4, A.2.6, A.2.7, A.2.9, A.2.14, A.2.18, and A.2.19);

c) A new section seven on Abstract Service Definition Conventions (see clauses 28-30).

Other changes are editorial and are related to the use of the revised ASN.1 notation, defined in ITU-T Recs. X.680-684 (1994) | ISO/IEC 8824:1994 and used in ITU-T Recs. X.500-525 (1993) | ISO/IEC 9596:1994.

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

The technical differences are as follows:

a) The use of the Universal Multiple-Octet Coded Character Set within OR-address attributes (see 18.2-18.4);

b) New Directory Context definitions (see A.4), and a Certificate Subject Alternative Name for MTAs (see A.5);

c) The addition of Annex H on Use of Protected Passwords for Message Store Access.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex K

Index

(This annex does not form an integral part of this Recommendation | International Standard)

This annex indexes this Specification. It gives the number(s) of the page(s) on which each item in each of several categories is defined. Its coverage of each category is exhaustive.

This annex indexes items (if any) in the following categories:

a) Abbreviations;

b) Terms;

c) Information items;

d) ASN.1 modules;

e) ASN.1 information object classes;

f) ASN.1 types;

g) ASN.1 values.

Abbreviations

A/SYS 30
AC 6
ACs 51
ACSE 6, 51
ADMD 32
AE 5
APDU 5
AS/SYS 30
ASE 5
ASEs 47
ASN.1 6
AST/SYS 30
AT/SYS 30
AU 10
C 7
COMPUSEC 19
D 7
DL 9
DSA 5
EIT 13
M 7
MASE 50
MD 31
MDSE 50
MHE 8
MHS 9
MRSE 49
MS 10
MSSE 49
MTA 11
MTS 10
MTSE 49
O 7
OSI 5
P1 51
P3 51
P7 51
PDAU 11
PDS 11
PRMD 32
RO 6
ROSE 6, 50
RT 6
RTSE 6, 51
S/SYS 30
ST/SYS 30
T/SYS 30
UA 10
UE 5

Terms

access and storage system 30
access and transfer system 30
access system 30
access unit 10
access, storage, and transfer system 30
actual recipient 15
administration management domain 32
administration-domain-name 37
affirmation 18
asymmetric 48
attribute 35
attribute list 35
attribute type 35
attribute value 35
common-name 37
conditional 7
consuming ASE 48
consuming UE 48
content 12
content type 12
conversion 18
country-name 37
defaultable 7
delivery 16
delivery agent 16

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

delivery report 13
described message 12
direct submission 16
direct user 9
distribution list 9
DL expansion 18
domain 31
domain-defined attribute 35
encoded information type 12
envelope 12
event 14
expansion point 18
explicit conversion 18
export 16
extension-physical-delivery-address-components 38
external routing 19
external transfer 16
formatted 43
Global MHS 32
grade 7
immediate recipient 14
implicit conversion 18
import 16
indirect submission 16
indirect user 9
intended recipient 15
internal routing 19
internal transfer 16
joining 17
local-postal-attributes 38
management domain 31
mandatory 7
member recipient 15
members 9
message 12
Message Handling 8
Message Handling Environment 8
Message Handling System 9
Message Storage 8
message store 10
Message Transfer 8
message transfer agent 11
Message Transfer System 10
messaging system 29
mnemonic OR-address 42
name resolution 18
nested 9
network-address 38
non-affirmation 18
non-delivery 18
non-delivery report 13
numeric OR-address 42
numeric-user-identifier 38
optional 7
OR-address 41
organizational-unit-names 39
organization-name 38
origination 15
originator 14
originator-specified alternate recipient 15
OR-name 34
pds-name 39
personal-name 39
Physical delivery 11
physical delivery access unit 11
physical delivery system 11
physical message 11
physical rendition 11
physical-delivery-country-name 39
physical-delivery-office-name 39
physical-delivery-office-number 39
physical-delivery-organization-name 39
physical-delivery-personal-name 39
postal OR-address 43
postal-code 40
poste-restante-address 40
post-office-box-address 40
potential recipient 15
private management domain 32
private-domain-name 40
probe 12
receipt 17
recipient 15
recipient-assigned alternate recipient 15
redirection 18
report 13
retrieval 16
routing 19
security policy 19
splitting 17
standard attribute 35
step 14
storage and transfer system 30
storage system 30
street-address 40
subject message 13
subject probe 13
submission 16
submission agent 16
submit permission 9
supplying ASE 48
supplying UE 48
symmetric 48
terminal OR-address 43
terminal-identifier 40
terminal-type 40
transfer 16
transfer system 30
transmittal 13
transmittal event 14
transmittal step 14
type 35
unformatted 43
unformatted-postal-address 40
unique-postal-name 41
user 9
user agent 10
value 35

Information items

address-capabilities-match 62
capability-match 63
DL Administrator Annotation 63
DL Nested DL 64
DL Policy 60
DL Reset Originator 64

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

DL Submit Permission 59
MHS Acceptable EITs 55
MHS Deliverable Classes 56
MHS Deliverable Content Types 56
MHS Distribution List 54
MHS DL Archive Service 56
MHS DL Members 56
MHS DL Policy 56
MHS DL Related Lists 57
MHS DL Submit Permissions 57
MHS DL Subscription Service 57
MHS Exclusively Acceptable EITs 57
MHS Maximum Content Length 57
MHS Message Store 54
MHS Message Store Directory Name 57
MHS Message Transfer Agent 54
MHS OR-Addresses 58
MHS OR-Addresses with Capabilities 58
MHS Supported Attributes 58
MHS Supported Automatic Actions 58
MHS Supported Content Types 58
MHS Supported Matching Rules 59
MHS Unacceptable EITs 59
MHS User 55
MHS User Agent 55
MTA Name 54
OR-Address 62
OR-Address with Capabilities 62
OR-name 63

ASN.1 modules

MHSDirectoryObjectsAndAttributes 67
MHSObjectIdentifiers 65

ASN.1 information object classes

ABSTRACT-ERROR 52
ABSTRACT-OPERATION 52
ATTRIBUTE 67
ATTRIBUTE (Directory) - see ISO/IEC 9594-2
ATTRIBUTE (MS) - see ISO/IEC 10021-5
AUTO-ACTION - see ISO/IEC 10021-5
CONTEXT - see ISO/IEC 9594-2
DIT-CONTEXT-USE-RULE - see ISO/IEC 9594-2
MATCHING-RULE - see ISO/IEC 9594-2
MHS-OBJECT 51
MS-ATTRIBUTE 67
OBJECT-CLASS - see ISO/IEC 9594-2
OTHER-NAME - see ISO/IEC 9594-8
PORT 52

ASN.1 types

AddressCapabilities 62, 72
AlgorithmIdentifier - see ISO/IEC 9594-8
AlgorithmInformation 61, 72
AttributeTable - see ISO/IEC 10021-5
AutoActionTable - see ISO/IEC 10021-5
Capability 62, 72
CertificateAssertion - see ISO/IEC 9594-8
ContentLength - see ISO/IEC 10021-4
DLPolicy 61, 72
DLSubmitPermission 59, 71
EncodedInformationTypesConstraints - see ISO/IEC 10021-4
ExtendedContentType - see ISO/IEC 10021-4
ExtendedEncodedInformationType - see ISO/IEC 10021-4
GlobalDomainIdentifier - see ISO/IEC 10021-4
ID 65
MatchingRuleTable - see ISO/IEC 10021-5
MTAName - see ISO/IEC 10021-4
Name - see ISO/IEC 9594-2
ORAddress - see ISO/IEC 10021-4
ORName - see ISO/IEC 10021-4
ORNamePattern 59, 71
RequestedDeliveryMethod - see ISO/IEC 10021-4
SecurityContext - see ISO/IEC 10021-4

ASN.1 values

addressCapabilitiesMatch 62, 73
any-user-may-submit 59, 71
applicationEntity - see ISO/IEC 9594-7
capabilityMatch 63, 73
commonName - see ISO/IEC 9594-6
description - see ISO/IEC 9594-6
distinguishedName - see ISO/IEC 9594-6
distinguishedNameMatch - see ISO/IEC 9594-2
dl-administrator-annotation 63, 73
dl-administrator-annotation-use-rule 63, 73
dl-nested-dl 64, 73
dl-nested-dl-use-rule 64, 73
dl-reset-originator 64, 73
dl-reset-originator-use-rule 64, 73
id-arch 65
id-at 65
id-at-encrypted-mhs-acceptable-eits 66
id-at-encrypted-mhs-deliverable-classes 66
id-at-encrypted-mhs-deliverable-content-types 66
id-at-encrypted-mhs-dl-archive-service 66
id-at-encrypted-mhs-dl-members 66
id-at-encrypted-mhs-dl-policy 66
id-at-encrypted-mhs-dl-related-lists 66
id-at-encrypted-mhs-dl-submit-permissions 66
id-at-encrypted-mhs-dl-subscription-service 66
id-at-encrypted-mhs-exclusively-acceptable-eits 66
id-at-encrypted-mhs-maximum-content-length 66
id-at-encrypted-mhs-message-store-dn 66
id-at-encrypted-mhs-or-addresses 66
id-at-encrypted-mhs-or-addresses-with-capabilities 66
id-at-encrypted-mhs-supported-attributes 66
id-at-encrypted-mhs-supported-automatic-actions 66
id-at-encrypted-mhs-supported-content-types 66
id-at-encrypted-mhs-supported-matching-rules 66
id-at-encrypted-mhs-unacceptable-eits 66
id-at-mhs-acceptable-eits 66
id-at-mhs-deliverable-classes 66
id-at-mhs-deliverable-content-types 66
id-at-mhs-dl-archive-service 66
id-at-mhs-dl-members 66
id-at-mhs-dl-policy 66
id-at-mhs-dl-related-lists 66
id-at-mhs-dl-submit-permissions 66
id-at-mhs-dl-subscription-service 66
id-at-mhs-exclusively-acceptable-eits 66

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

id-at-mhs-maximum-content-length 66
id-at-mhs-message-store-dn 66
id-at-mhs-or-addresses 66
id-at-mhs-or-addresses-with-capabilities 66
id-at-mhs-supported-attributes 66
id-at-mhs-supported-automatic-actions 66
id-at-mhs-supported-content-types 66
id-at-mhs-supported-matching-rules 66
id-at-mhs-unacceptable-eits 66
id-con 65
id-con-dl-administrator-annotation 66
id-con-dl-nested-dl 66
id-con-dl-reset-originator 66
id-directory-objects-and-attributes 65
id-edims 65
id-group 65
id-ipms 65
id-management 65
id-mhs-protocols 65
id-mod 65
id-mr 65
id-mr-address-capabilities-match 66
id-mr-capability-match 66
id-mr-orname-exact-match 66
id-ms 65
id-mts 65
id-object-identifiers 65
id-oc 65
id-oc-mhs-distribution-list 66
id-oc-mhs-message-store 66
id-oc-mhs-message-transfer-agent 66
id-oc-mhs-user 66
id-oc-mhs-user-agent 66
id-routing 65
id-san 65
id-san-mta-name 66
integerMatch - see ISO/IEC 9594-6
mhs-acceptable-eits 55, 69
mhs-deliverable-classes 56, 69
mhs-deliverable-content-types 56, 69
mhs-distribution-list 54, 68
mhs-dl-archive-service 56, 70
mhs-dl-members 56, 70
mhs-dl-policy 56, 70
mhs-dl-related-lists 57, 70
mhs-dl-submit-permissions 57, 70
mhs-dl-subscription-service 57, 70
mhs-exclusively-acceptable-eits 57, 70
mhs-maximum-content-length 57, 70
mhs-message-store 54, 69
mhs-message-store-dn 58, 70
mhs-message-transfer-agent 55, 69
mhs-or-addresses 58, 71
mhs-or-addresses-with-capabilities 58, 71
mhs-supported-attributes 58, 71
mhs-supported-automatic-actions 58, 71
mhs-supported-content-types 58, 71
mhs-supported-matching-rules 59, 71
mhs-unacceptable-eits 59, 71
mhs-user 55, 69
mhs-user-agent 55, 69
mta-name 64, 73
objectIdentifierMatch - see ISO/IEC 9594-2
oRAddressElementsMatch - see ISO/IEC 10021-5
oRAddressMatch - see ISO/IEC 10021-5
oRAddressSubstringElementsMatch - see ISO/IEC 10021-5
organizationalUnitName - see ISO/IEC 9594-6
organizationName - see ISO/IEC 9594-6
oRNameElementsMatch - see ISO/IEC 10021-5
oRNameExactMatch 63, 73
oRNameMatch - see ISO/IEC 10021-5
oRNameSingleElementMatch - see ISO/IEC 10021-5
oRNameSubstringElementsMatch - see ISO/IEC 10021-5
owner - see ISO/IEC 9594-6
protocolInformation - see ISO/IEC 9594-6
seeAlso - see ISO/IEC 9594-6
top - see ISO/IEC 9594-2

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

ICS 35.240.20

Price based on 95 pages

--`,,,`-`-`,,`,,`,`,,`---

© ISO/IEC 2003 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale