

AS/NZS 4033.2:1999

ISO/IEC 10021-2:1996

ISO/IEC 10021-2:1996/Cor.1:1998

AS/NZS 4033.2

Australian/New Zealand Standard™

**Information technology—Text
communication—Message-oriented text
interchange systems**

Part 2: Overall architecture



Standards Australia



STANDARDS
Documents

Document Sharing Hub

AS/NZS 4033.2:1999

This Joint Australian/New Zealand Standard was prepared by Joint Technical Committee IT/1, Information Systems—Interconnection. It was approved on behalf of the Council of Standards Australia on 14 July 1999 and on behalf of the Council of Standards New Zealand on 28 June 1999. It was published on 5 August 1999.

The following interests are represented on Committee IT/1:

Australian Association of Chief Information Officers
Australian Association of Permanent Building Societies
Australian Bankers Association
Australian Bureau of Statistics
Australian Chamber of Commerce and Industry
Australian Communications Industry Forum
Australian Computer Society
Australian Information Industry Association
Australian Telecommunications Users Group
Australian Vice-Chancellors Committee
CSIRO Mathematical and Information Sciences
Department of Communications and the Arts
Department of Industry Science and Tourism (Commonwealth)
Electrical Compliance Testing Association
Telecom New Zealand
Telstra Corporation

Review of Standards. To keep abreast of progress in industry, Joint Australian/New Zealand Standards are subject to periodic review and are kept up to date by the issue of amendments or new editions as necessary. It is important therefore that Standards users ensure that they are in possession of the latest edition, and any amendments thereto.

Full details of all Joint Standards and related publications will be found in the Standards Australia and Standards New Zealand Catalogue of Publications; this information is supplemented each month by the magazines 'The Australian Standard' and 'Standards New Zealand', which subscribing members receive, and which give details of new publications, new editions and amendments, and of withdrawn Standards.

Suggestions for improvements to Joint Standards, addressed to the head office of either Standards Australia or Standards New Zealand, are welcomed. Notification of any inaccuracy or ambiguity found in a Joint Australian/New Zealand Standard should be made without delay in order that the matter may be investigated and appropriate action taken.

This Standard was issued in draft form for comment as DR 99174.

AS/NZS 4033.2:1999

Australian/New Zealand Standard™

**Information technology—Text
communication—Message-oriented text
interchange systems**

Part 2: Overall architecture

Originated in Australia as AS 4033.2—1992.
Jointly revised and designated AS/NZS 4033.2:1999.

Published jointly by:

Standards Australia
1 The Crescent,
Homebush NSW 2140 Australia

Standards New Zealand
Level 10, Radio New Zealand House,
155 The Terrace,
Wellington 6001 New Zealand

PREFACE

This Standard was prepared by the Joint Standards Australia/Standards New Zealand Committee IT/1, Information Systems—Interconnection, to supersede AS 4033.2—1992. This Standard is identical with and has been reproduced from ISO/IEC 10021-2:1996, *Information technology—Message Handling Systems (MHS): Overall architecture* and its Technical Corrigendum 1: 1998.

The objective of this Standard is to provide network designers with a definition of the overall architecture of a message handling system including abstract models, various configurations and naming and addressing issues.

As this Standard is reproduced from an International Standard, the following applies:

- (a) Its number does not appear on each page of text and its identity is shown only on the cover and title page.
- (b) In the source text 'this Recommendation/International Standard' should read 'this Australian/New Zealand Standard'.
- (c) A full point should be substituted for a comma when referring to a decimal marker.

© Copyright – STANDARDS AUSTRALIA/STANDARDS NEW ZEALAND

Users of Standards are reminded that copyright subsists in all Standards Australia and Standards New Zealand publications and software. Except where the Copyright Act allows and except where provided for below no publications or software produced by Standards Australia or Standards New Zealand may be reproduced, stored in a retrieval system in any form or transmitted by any means without prior permission in writing from Standards Australia or Standards New Zealand. Permission may be conditional on an appropriate royalty payment. Australian requests for permission and information on commercial software royalties should be directed to the head office of Standards Australia. New Zealand requests should be directed to Standards New Zealand.

Up to 10 percent of the technical content pages of a Standard may be copied for use exclusively in-house by purchasers of the Standard without payment of a royalty or advice to Standards Australia or Standards New Zealand.

Inclusion of copyright material in computer software programs is also permitted without royalty payment provided such programs are used exclusively in-house by the creators of the programs.

Care should be taken to ensure that material used is from the current edition of the Standard and that it is updated whenever the Standard is amended or revised. The number and date of the Standard should therefore be clearly identified.

The use of material in print form or in computer software programs to be used commercially, with or without payment, or in commercial contracts is subject to the payment of a royalty. This policy may be varied by Standards Australia or Standards New Zealand at any time.



CONTENTS

	<i>Page</i>
SECTION 1 – INTRODUCTION	1
1 Scope	1
2 Normative references	3
2.1 Open Systems Interconnection	3
2.1.1 Identical Recommendations International Standards	3
2.1.2 Paired Recommendations International Standards equivalent in technical content	4
2.1.3 Additional references	4
2.2 Directory Systems	4
2.2.1 Identical Recommendations International Standards	4
2.3 Message Handling Systems	4
2.3.1 Identical Recommendations International Standards	5
2.3.2 Paired Recommendations International Standards equivalent in technical content	5
2.3.3 Additional References	5
2.4 Country Codes	5
2.5 Network Addresses	5
3 Definitions	5
3.1 Open Systems Interconnection	6
3.2 Directory Systems	7
3.3 Message Handling Systems	7
4 Abbreviations	7
5 Conventions	7
5.1 ASN.1	7
5.2 Grade	8
5.3 Terms	8
SECTION 2 – ABSTRACT MODELS	8
6 Overview	8
7 Functional model	8
7.1 Primary functional objects	9
7.1.1 The Message Handling System	9
7.1.2 Users	9
7.1.3 Distribution lists	10
7.2 Secondary functional objects	10
7.2.1 The Message Transfer System	10
7.2.2 User Agents	11

7.2.3	Message stores	11
7.2.4	Access units	11
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	12
7.4.3	Telex	12
8	Information model	12
8.1	Messages	12
8.2	Probes	13
8.3	Reports	14
9	Operational model	14
9.1	Transmittal	14
9.2	Transmittal roles	14
9.3	Transmittal steps	16
9.3.1	Origination	16
9.3.2	Submission	16
9.3.3	Import	17
9.3.4	Transfer	17
9.3.5	Export	17
9.3.6	Delivery	17
9.3.7	Retrieval	17
9.3.8	Receipt	17
9.4	Transmittal events	17
9.4.1	Splitting	18
9.4.2	Joining	18
9.4.3	Name resolution	18
9.4.4	DL expansion	18
9.4.5	Redirection	18
9.4.6	Conversion	19
9.4.7	Non-delivery	19
9.4.8	Non-affirmation	19
9.4.9	Affirmation	19
9.4.10	Routing	19
10	Security model	19
10.1	Security policies	20
10.2	Security services	20
10.2.1	Origin Authentication security services	20
10.2.1.1	Data Origin Authentication security services	20
10.2.1.2	Proof of Submission security service	22
10.2.1.3	Proof of Delivery security service	22
10.2.2	Secure Access Management security service	22
10.2.2.1	Peer Entity Authentication security service	22
10.2.2.2	Security Context security service	22
10.2.3	Data Confidentiality security services	22
10.2.3.1	Connection Confidentiality security service	23
10.2.3.2	Content Confidentiality security service	23
10.2.3.3	Message Flow Confidentiality security service	23
10.2.4	Data Integrity security services	23
10.2.4.1	Connection Integrity security service	23
10.2.4.2	Content Integrity security service	23
10.2.4.3	Message Sequence Integrity security service	23
10.2.5	Non-Repudiation security services	24

	<i>Page</i>
10.2.5.1 Non-Repudiation of Origin security service	24
10.2.5.2 Non-Repudiation of Submission security service	24
10.2.5.3 Non-Repudiation of Delivery security service	24
10.2.6 Message Security Labelling security service	24
10.2.7 Security management services	24
10.2.7.1 Change Credentials security service	24
10.2.7.2 Register security service	25
10.2.7.3 MS-Register security service	25
10.3 Security elements	25
10.3.1 Authentication security elements	25
10.3.1.1 Authentication Exchange security element	25
10.3.1.2 Data Origin Authentication security elements	25
10.3.1.3 Proof of Submission security element	26
10.3.1.4 Proof of Delivery security element	26
10.3.2 Secure Access Management security elements	26
10.3.2.1 Security Context security element	26
10.3.2.2 Register security element	26
10.3.2.3 MS-Register security element	27
10.3.3 Data Confidentiality security elements	27
10.3.3.1 Content Confidentiality security element	27
10.3.3.2 Message Argument Confidentiality security element	27
10.3.4 Data Integrity security elements	27
10.3.4.1 Content Integrity security element	27
10.3.4.2 Message Argument Integrity security element	27
10.3.4.3 Message Sequence Integrity security element	28
10.3.5 Non-Repudiation security elements	28
10.3.6 Security Label security elements	28
10.3.6.1 Message Security Label security element	28
10.3.7 Security Management security elements	28
10.3.7.1 Change Credentials security element	28
10.3.8 Double Enveloping Technique	28
10.3.9 Encoding for encryption and hashing	28
SECTION 3 – CONFIGURATIONS	29
11 Overview	29
12 Functional configurations	29
12.1 Regarding the Directory	29
12.2 Regarding the Message Store	29
13 Physical configurations	30
13.1 Messaging Systems	30
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	32
13.2.1 Fully centralized	32
13.2.2 Centralized Message Transfer and Storage	32
13.2.3 Centralized Message Transfer	32
13.2.4 Fully distributed	32
14 Organizational configurations	33

14.1	Management domains	33
14.1.1	Administration management domains.....	33
14.1.2	Private management domains	33
14.2	Representative configurations.....	33
14.2.1	Fully centralized.....	34
14.2.2	Directly connected	34
14.2.3	Indirectly connected.....	34
15	The Global MHS.....	34
SECTION 4 – NAMING, ADDRESSING, AND ROUTING		35
16	Overview	35
17	Naming.....	35
17.1	Directory names	35
17.2	OR-Names.....	36
18	Addressing	36
18.1	Attribute lists.....	36
18.2	Character sets	36
18.3	Standard attributes	36
18.3.1	Administration-domain-name	38
18.3.2	Common-name.....	39
18.3.3	Country-name	39
18.3.4	Extension-postal-O/R-address-components.....	39
18.3.5	Extension-physical-delivery-address-components.....	39
18.3.6	Local-postal-attributes	39
18.3.7	Network-address	39
18.3.8	Numeric-user-identifier.....	40
18.3.9	Organization-name.....	40
18.3.10	Organizational-unit-names.....	40
18.3.11	Pds-name.....	40
18.3.12	Personal-name.....	40
18.3.13	Physical-delivery-country-name	40
18.3.14	Physical-delivery-office-name	41
18.3.15	Physical-delivery-office-number	41
18.3.16	Physical-delivery-organization-name	41
18.3.17	Physical-delivery-personal-name.....	41
18.3.18	Post-office-box-address	41
18.3.19	Postal-code.....	41
18.3.20	Poste-restante-address.....	41
18.3.21	Private-domain-name	41
18.3.22	Street-address	41
18.3.23	Terminal-identifier.....	42
18.3.24	Terminal-type.....	42
18.3.25	Unformatted-postal-address	42
18.3.26	Unique-postal-name.....	42
18.4	Attribute list equivalence	42
18.5	OR-Address Forms	42
18.5.1	Mnemonic OR-address	44
18.5.2	Numeric OR-address.....	44
18.5.3	Postal OR-address.....	44
18.5.4	Terminal OR-address	44
18.5.5	Determination of address forms	45
18.6	Conditional attributes.....	45

	<i>Page</i>
19 Routing.....	45
SECTION 5 – USE OF THE DIRECTORY	47
20 Overview	47
21 Authentication	47
22 Name resolution	47
23 DL expansion	47
24 Capability assessment	47
SECTION 6 – OSI REALIZATION	48
25 Overview	48
26 Application service elements.....	48
26.1 The ASE concept	48
26.2 Symmetric and Asymmetric ASEs.....	48
26.3 Message Handling ASEs.....	51
26.3.1 Message Transfer	51
26.3.2 Message Submission	51
26.3.3 Message Delivery.....	51
26.3.4 Message Retrieval	51
26.3.5 Message Administration	51
26.4 Supporting ASEs.....	51
26.4.1 Remote Operations.....	52
26.4.2 Reliable Transfer.....	52
26.4.3 Association Control	52
27 Application contexts.....	52
SECTION 7 – ABSTRACT SERVICE DEFINITION CONVENTIONS.....	53
28 Overview	53
29 Components of the Abstract model	53
29.1 Abstract objects	53
29.2 Abstract contracts.....	53
29.3 Connection packages	53
29.4 Abstract ports	54
29.5 Abstract operations and Abstract errors.....	54
30 ROS realization	54
Annex A – Directory object classes and attributes	55
A.1 Object classes.....	55
A.1.1 MHS Distribution List	55
A.1.2 MHS Message Store	55
A.1.3 MHS Message Transfer Agent.....	56
A.1.4 MHS User	56
A.1.5 MHS User Agent.....	56
A.2 Attributes.....	56
A.2.1 MHS Acceptable EITs	57
A.2.2 MHS Deliverable Classes	57
A.2.3 MHS Deliverable Content Types.....	57
A.2.4 MHS DL Archive Service.....	57
A.2.5 MHS DL Members	57
A.2.6 MHS DL Policy	58
A.2.7 MHS DL Related Lists.....	58
A.2.8 MHS DL Submit Permissions.....	58
A.2.9 MHS DL Subscription Service	58

A.2.10	MHS Exclusively Acceptable EITs	58
A.2.11	MHS Maximum Content Length	59
A.2.12	MHS Message Store Directory Name.....	59
A.2.13	MHS OR-Addresses.....	59
A.2.14	MHS OR-Addresses with Capabilities.....	59
A.2.15	MHS Supported Attributes	59
A.2.16	MHS Supported Automatic Actions	60
A.2.17	MHS Supported Content Types	60
A.2.18	MHS Supported Matching Rules	60
A.2.19	MHS Unacceptable EITs	60
A.3	Attribute syntaxes	60
A.3.1	DL Submit Permission	60
A.3.1.1	Procedure for evaluating DL Submit Permission.....	61
A.3.1.2	Procedure for determining equivalence of OR-Names	61
A.3.2	DL Policy	62
A.3.3	OR-Address	63
A.3.4	OR-Address with Capabilities	63
A.3.5	OR-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.....	73
D.1	Masquerade	73
D.2	Message sequencing.....	73
D.3	Modification of information.....	74
D.4	Denial of service	75
D.5	Repudiation	75
D.6	Leakage of Information.....	75
D.7	Other threats.....	75
Annex E	– Provision of security services in ITU-T Rec. X.411 ISO/IEC 10021-4	76
Annex F	– Representation of OR-addresses for human usage	77
F.1	Purpose.....	77
F.2	Scope.....	77
F.3	Format.....	77
F.3.1	General	77
F.3.2	Labelled format	78
F.3.2.1	Syntax	78
F.3.2.2	Terminal-type.....	79
F.3.2.3	Domain-defined attribute	79
F.3.3	Self-explanatory format	80
F.4	User interface	80
F.4.1	Examples of application.....	81
Annex G	– Use of OR-addresses by multinational organizations	82
G.1	Addressing principles.....	82
G.2	Example configurations	83
G.2.1	Multiple independent PRMDs	83
G.2.2	A single PRMD, named from a "home" country	84
G.2.3	A single PRMD with multiple country and domain names	84
G.3	Alias OR-addresses	85
Annex H	– Differences between ISO/IEC 10021-2 and ITU-T Rec. X.402	86
Annex I	– Summary of changes to previous editions.....	87
I.1	Differences between ISO/IEC 10021-2:1990 and CCITT Rec. X.402 (1992)	87
I.2	Differences between CCITT Rec. X.402 (1992) and ITU-T Rec. X.402 (1995) ISO/IEC 10021-2:1996	87

AUSTRALIAN/NEW ZEALAND STANDARD

**Information technology—Text communication—
Message-oriented text interchange systems****Part 2:
Overall architecture****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 ITU-T Recommendations | 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 Recommendation X.403. The detailed rules by which the MTS converts the contents of messages from one EIT to another are defined in Recommendation 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 Recommendation T.330. The EDI Messaging Service is described in CCITT Rec. F.435 and ISO/IEC 10021-8, and the EDI Messaging System, another application of Message Handling, is defined in CCITT Rec. X.435 and 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.

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.

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/IEC 7498-1. 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 CCITT Rec. X.227 | ISO/IEC 8650-1. The means for reliably conveying APDUs over associations, the RTSE, is defined in ITU-T Rec. X.218 and ISO/IEC 9066-1 and CCITT Rec. X.228 and 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.

This Recommendation | International Standard is structured as follows. Section 1 gives a general overview. Section 2 presents abstract models of Message Handling. Section 3 specifies how one can configure the MHS to satisfy any of a variety of functional, physical, and organizational requirements. Section 4 describes the naming and addressing of users and distribution lists and the routing of information objects to them. Section 5 describes the uses the MHS may make of the Directory. Section 6 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 7. Annexes provide important supplemental information.

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

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.403	Conformance testing
–	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	–	MHS Routing
MHS Management		
11588-1	X.460	Management: Model and Architecture
11588-3	X.462	Logging Information
11588-8	X.467	Message Transfer Agent Management

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

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

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 edition of the Recommendations and Standards listed below. Members of ISO and IEC maintain registers of currently valid International Standards. The Telecommunication Standardization Bureau of the 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.

2.1.1 Identical Recommendations | International Standards

- ITU-T Recommendation X.200 (1994 | ISO/IEC 7498-1:1994, *Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model*.
- ITU-T Recommendation X.216 (1994) | ISO/IEC 8822:1994, *Information technology – Open Systems Interconnection – 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.227 (1995) | ISO/IEC 8650-1:1996, *Information technology – Open Systems Interconnection – Connection-oriented protocol for the Association Control Service Element: Protocol specification*.
- ITU-T Recommendation X.680 (1994) | ISO/IEC 8824-1:1995, *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation*.
- ITU-T Recommendation X.681 (1994) | ISO/IEC 8824-2:1995, *Information technology – Abstract Syntax Notation One (ASN.1): Information object specification*.

- ITU-T Recommendation X.682 (1994) | ISO/IEC 8824-3:1995, *Information technology – Abstract Syntax Notation One (ASN.1): Constraint specification.*
- ITU-T Recommendation X.683 (1994) | ISO/IEC 8824-4:1995, *Information technology – Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications.*
- ITU-T Recommendation X.690 (1994) | ISO/IEC 8825-1:1995, *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 realizations – Remote Operations Service Element (ROSE) service definition.*
- ITU-T Recommendation X.882 (1994) | ISO/IEC 13712-3:1995, *Information technology – Remote Operations: OSI realizations: Remote Operations Service Element (ROSE) protocol specification.*

2.1.2 Paired Recommendations | International Standards equivalent in technical content

- 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.*
- 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.*

2.1.3 Additional references

- ISO 7498-2:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture.*

2.2 Directory Systems

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

2.2.1 Identical Recommendations | International Standards

- ITU-T Recommendation X.500 (1993) | ISO/IEC 9594-1:1995, *Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models, and services.*
- ITU-T Recommendation X.501 (1993) | ISO/IEC 9594-2:1995, *Information technology – Open Systems Interconnection – The Directory: Models.*
- ITU-T Recommendation X.509 (1993) | ISO/IEC 9594-8:1995, *Information technology – Open Systems Interconnection – The Directory: Authentication framework.*
- ITU-T Recommendation X.511 (1993) | ISO/IEC 9594-3:1995, *Information technology – Open Systems Interconnection – The Directory: Abstract service definition.*
- ITU-T Recommendation X.518 (1993) | ISO/IEC 9594-4:1995, *Information technology – Open Systems Interconnection – The Directory: Procedures for distributed operation.*
- ITU-T Recommendation X.519 (1993) | ISO/IEC 9594-5:1995, *Information technology – Open Systems Interconnection – The Directory: Protocol specifications.*
- ITU-T Recommendation X.520 (1993) | ISO/IEC 9594-6:1995, *Information technology – Open Systems Interconnection – The Directory: Selected attribute types.*
- ITU-T Recommendation X.521 (1993) | ISO/IEC 9594-7:1995, *Information technology – Open Systems Interconnection – The Directory: Selected object classes.*
- ITU-T Recommendation X.525 (1993) | ISO/IEC 9594-9:1995, *Information technology – Open Systems Interconnection – The Directory: Replication.*

2.3 Message Handling Systems

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

2.3.1 Identical Recommendations | International Standards

- ITU-T Recommendation X.411 (1995) | ISO/IEC 10021-4:1996, *Information technology – Message Handling Systems (MHS): Message transfer system – Abstract service definition and procedures.*
- ITU-T Recommendation X.413 (1995) | ISO/IEC 10021-5:1996, *Information technology – Message Handling Systems (MHS): Message store: Abstract service definition.*
- ITU-T Recommendation X.419 (1995) | ISO/IEC 10021-6:1996, *Information technology – Message Handling Systems (MHS): Protocol specifications.*
- ITU-T Recommendation X.420 (1996) | ISO/IEC 10021-7:1996, *Information technology – Message Handling Systems (MHS): Interpersonal messaging system.*
- ITU-T Recommendation X.460 (1995) | ISO/IEC 11588-1:1996, *Information technology – Message Handling Systems (MHS) management: Model and architecture.*
- ITU-T Recommendation X.462¹⁾ | ISO/IEC 11588-3:...¹⁾, *Information technology – Message Handling Systems (MHS) management: Logging information.*
- ITU-T Recommendation X.467¹⁾ | ISO/IEC 11588-8:...¹⁾, *Information technology – Message Handling Systems (MHS) management: Message transfer agent management.*

2.3.2 Paired Recommendations | International Standards equivalent in technical content

- ITU-T Recommendation F.400/X.400 (1993), *Message handling services: Message handling system and service overview.*
ISO/IEC 10021-1:1990, *Information technology – Text Communication – Message-Oriented Text Interchange Systems (MOTIS) – Part 1: System and Service Overview.*
- CCITT Recommendation F.435 (1991), *Message handling: Electronic data interchange messaging service.*
ISO/IEC 10021-8:1995, *Information technology – Message Handling Systems (MHS) – Part 8: Electronic Data Interchange Messaging Service.*
- CCITT Recommendation X.435 (1991), *Message Handling Systems: Electronic data interchange messaging system.*
ISO/IEC 10021-9:1995, *Information technology – Message Handling Systems (MHS) – Part 9: Electronic Data Interchange Messaging System.*

2.3.3 Additional References

- CCITT Recommendation T.330 (1988), *Telematic access to interpersonal messaging system.*
- CCITT Recommendation X.408 (1988), *Message handling systems: Encoded information type conversion rules.*
- ISO/IEC 10021-10:...¹⁾, *Information technology – Message Handling Systems (MHS) – Part 10: MHS Routing.*

2.4 Country Codes

This Specification cites the following Country Code specifications:

- ISO 3166:1993, *Codes for the representation of names of countries.*
- CCITT Recommendation X.121 (1992), *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.*

3 Definitions

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

¹⁾ Presently at the stage of draft.

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 Systems Interconnection (OSI);
- i) peer;
- j) presentation context;
- k) protocol;
- l) Reference Model;
- m) transfer syntax; and
- n) User Element (UE).

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 and 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 (ROs);
- h) Remote Operations Service Element (ROSE);
- i) result;
- j) synchronous; and
- k) unbind.

3.2 Directory Systems

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

- a) attribute;
- b) certificate;
- c) certification authority;
- d) certification path;
- e) directory entry; entry;
- f) Directory System Agent (DSA);
- g) Directory;
- h) hash function;
- i) name;
- j) object class;
- k) object;
- l) simple authentication; and
- m) strong authentication.

3.3 Message Handling Systems

For the purposes of this Specification the terms indexed in Annex J apply.

4 Abbreviations

For the purposes of this Specification the abbreviations indexed in Annex J 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.

5.2 Grade

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

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

5.3 Terms

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

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

SECTION 2 – ABSTRACT MODELS

6 Overview

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

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

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

This Section covers the following topics:

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

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

7 Functional model

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

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

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

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

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

7.1 Primary functional objects

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

The situation is depicted in Figure 1.

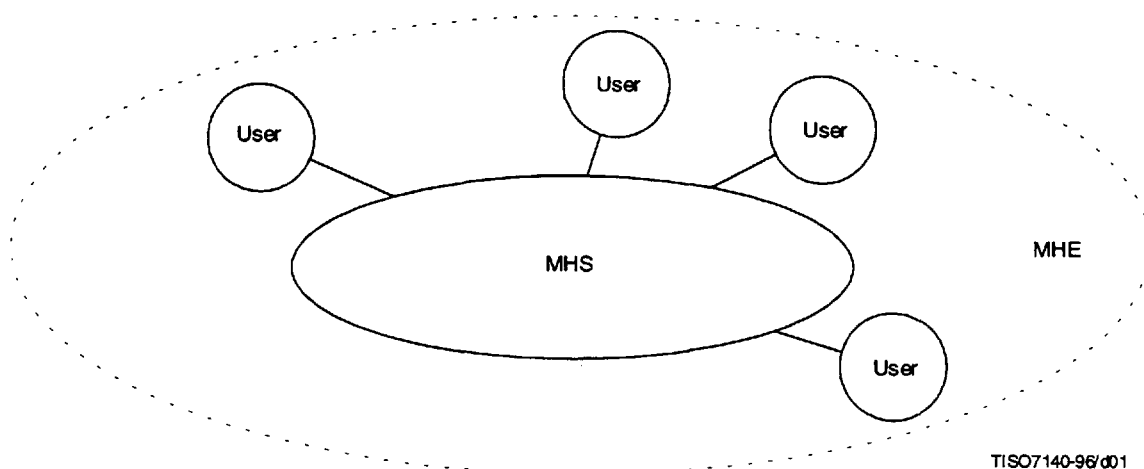


Figure 1 – The Message Handling environment

7.1.1 The Message Handling System

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

The MHE comprises a single MHS.

7.1.2 Users

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

The following kinds of user are distinguished:

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

The MHE comprises any number of users.

7.1.3 Distribution lists

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

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

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

The MHE comprises any number of DLs.

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

7.2 Secondary functional objects

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

The situation is depicted in Figure 2.

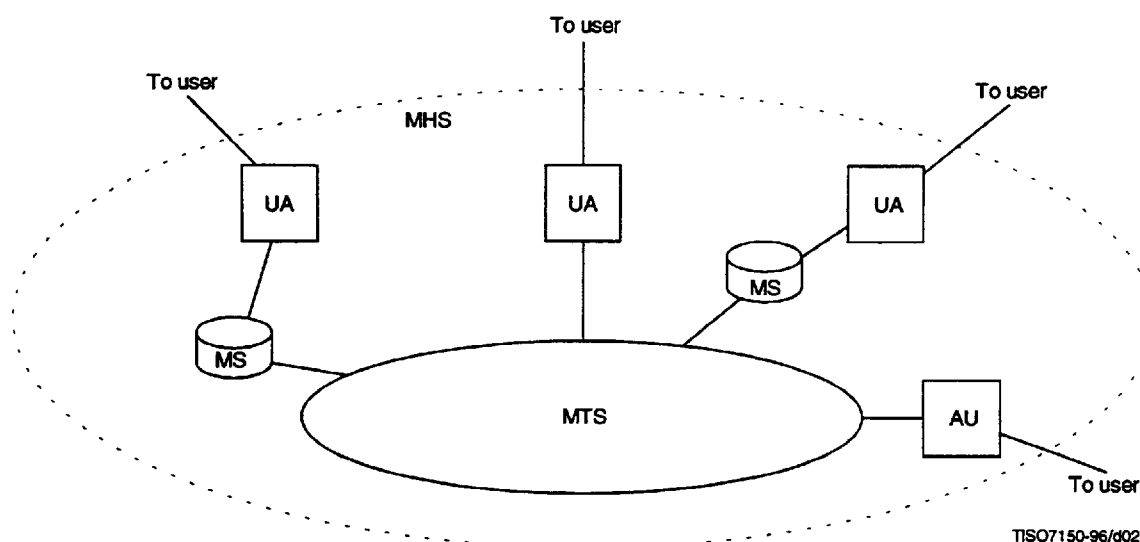


Figure 2 – The Message Handling System

7.2.1 The Message Transfer System

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

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

The MHS comprises a single MTS.

7.2.2 User Agents

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

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

The MHS comprises any number of UAs.

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

7.2.3 Message stores

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

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

The MHS comprises any number of MSs.

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

7.2.4 Access units

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

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

The MHS comprises any number of AUs.

7.3 Tertiary functional objects

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

The situation is depicted in Figure 3.

7.3.1 Message Transfer Agents

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

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

The MTS comprises any number of MTAs.

7.4 Selected AU types

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

7.4.1 Physical delivery

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

The transformation of a *message* 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*.

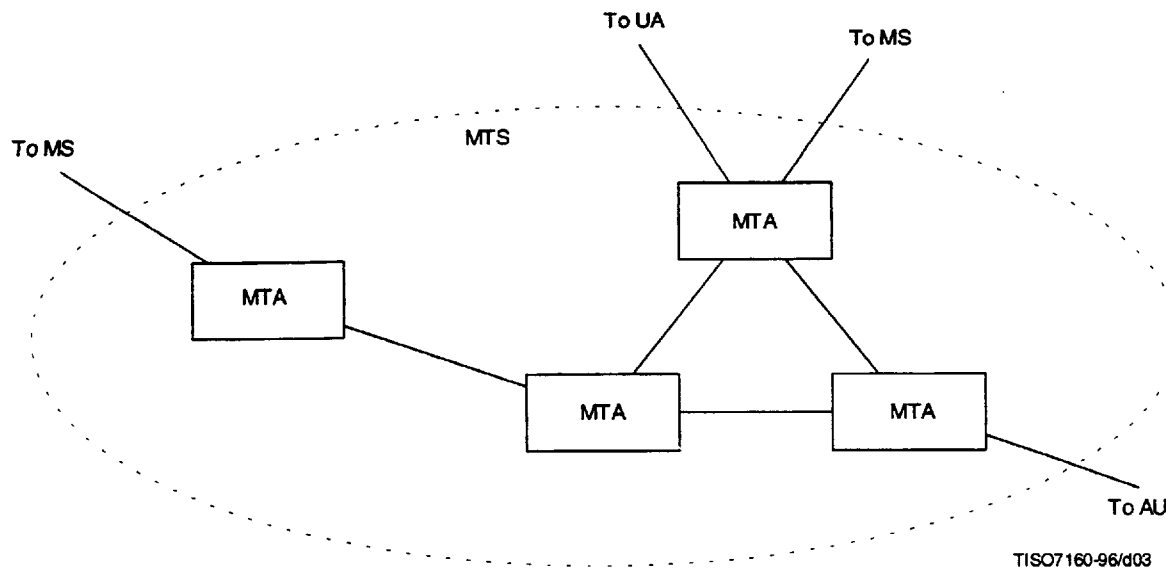


Figure 3 – The Message Transfer System

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

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

7.4.2 Telematic

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

7.4.3 Telex

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

8 Information model

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

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

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:

- 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*.
- content:** An information object that the MTS neither examines nor modifies, except for *conversion*, during its conveyance of the message.

Table 4 – Conveyable information objects

Information object	Functional object				
	User	UA	MS	MTA	AU
Message	SD	–	–	–	–
Probe	S	–	–	D	–
Report	D	–	–	S	–
S Ultimate source					
D Ultimate destination					

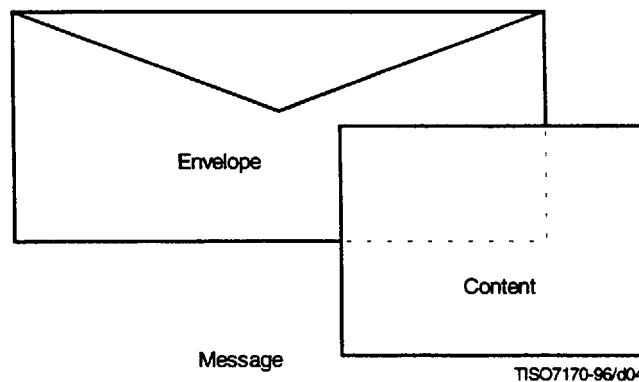


Figure 4 – A Message's Envelope and Content

One piece of information borne by the envelope identifies the type of the content. The **content type** is an identifier (an ASN.1 Object Identifier or Integer) that denotes the syntax and semantics of the content overall. This identifier enables the MTS to determine the message's *deliverability* to particular users, and enables UAs and MSs to interpret and process the content.

Another piece of information borne by the envelope identifies the types of encoded information represented in the content. An **encoded information type (EIT)** is an identifier that denotes the medium and format (e.g. IAS 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, export, or affirmation* of the subject message or probe, or *DL expansion*.
- b) **non-delivery report:** *Non-delivery or non-affirmation* of the subject message or probe.

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

9 Operational model

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

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

9.1 Transmittal

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

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

The information flow of transmittal is depicted in Figure 5. This 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.

Figure 5 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*.

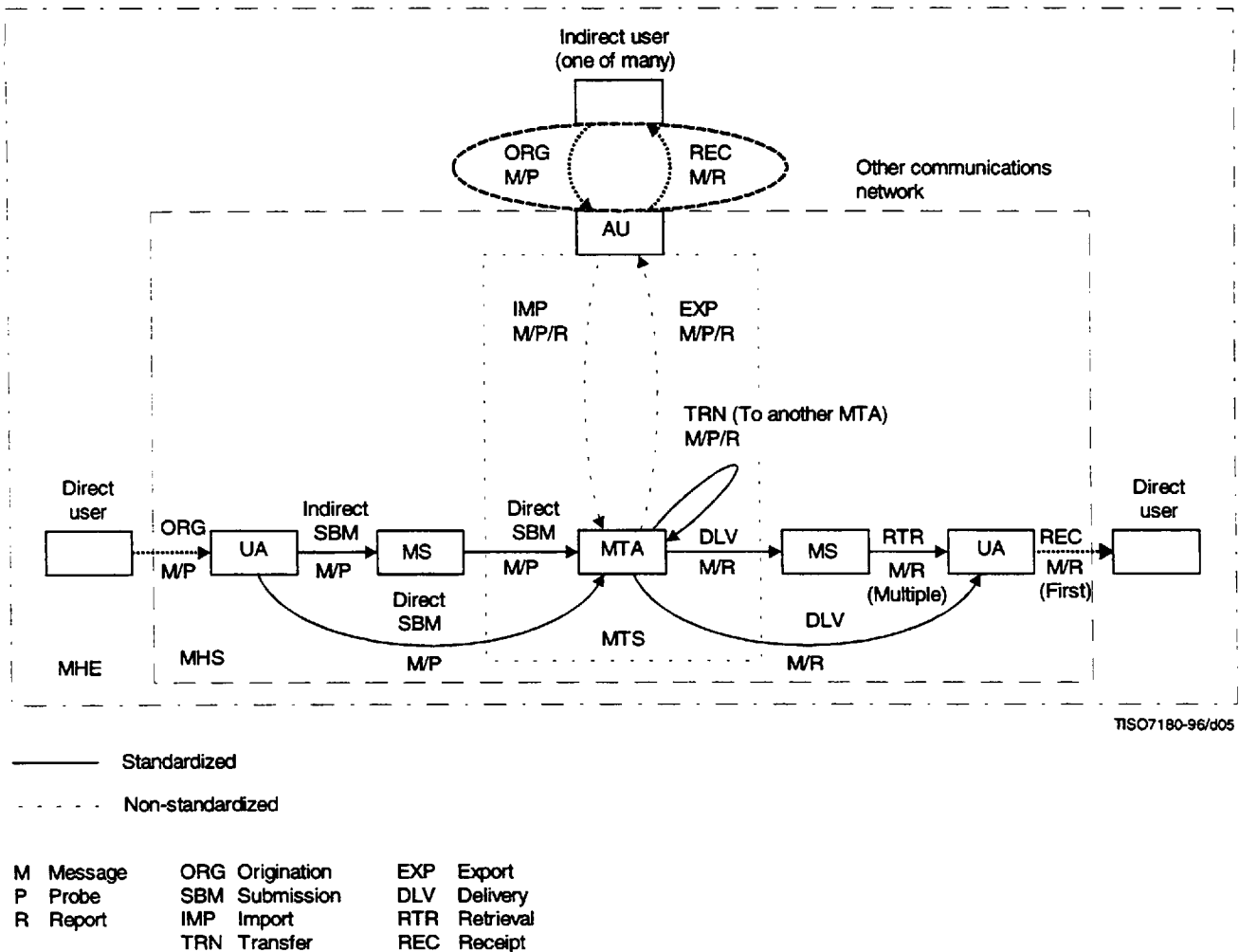
One event plays a distinguished role in transmittal. *Splitting* replicates a message or probe and divides responsibility for its *immediate recipients* among the resulting information objects. The potential recipients associated with a particular instance of a message or probe are called the **immediate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

9.2 Transmittal roles

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

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

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



TIS07180-96/d05

Figure 5 – The information flow of transmittal

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

- intended recipient:** One of the users and DLs the originator specifies as a message’s or probe’s intended destinations.
- 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.
- member recipient:** A user or DL to which a message (but not a probe) is conveyed as a result of *DL expansion*.
- 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:

- 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.
- 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.

Table 5 – Transmittal steps

Transmittal step	Standardized?	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	–	–	–	–	D	S
Transfer	Yes	X	X	–	–	–	–	SD	–
Export	No	X	X	–	–	–	–	S	D
Delivery	Yes	X	–	–	–	D	D	S	–
Retrieval	Yes	X	–	–	–	D	S	–	–
Receipt	No	X	–	–	D	S	–	–	–
M Message S Source P Probe D Destination R Report X Permitted									

Table 5 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.

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

9.3.1 Origination

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

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

9.3.2 Submission

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

- 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.

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

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

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

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

9.3.3 Import

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

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

9.3.4 Transfer

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

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

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

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

9.3.5 Export

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

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

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

9.3.6 Delivery

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

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

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

9.3.7 Retrieval

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

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

9.3.8 Receipt

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

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

9.4 Transmittal events

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

All the events occur within the MTS.

The kinds of transmittal events, summarized in Table 6, are individually defined and described in the subclauses below.

Table 6 – Transmittal events

Transmittal event	Information objects			Functional objects				
	M	P	R	User	UA	MS	MTA	AU
Splitting	X	X	–	–	–	–	X	–
Joining	X	X	X	–	–	–	X	–
Name resolution	X	X	–	–	–	–	X	–
DL expansion	X	–	–	–	–	–	X	–
Redirection	X	X	–	–	–	–	X	–
Conversion	X	X	–	–	–	–	X	–
Non-delivery	X	–	X	–	–	–	X	–
Non-affirmation	–	X	–	–	–	–	X	–
Affirmation	–	X	–	–	–	–	X	–
Routing	X	X	X	–	–	–	X	–
M Message P Probe R Report X Permitted								

9.4.1 Splitting

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

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

9.4.2 Joining

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

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

9.4.3 Name resolution

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

9.4.4 DL expansion

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

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

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

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

9.4.5 Redirection

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

9.4.6 Conversion

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

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

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

9.4.7 Non-delivery

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

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

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

9.4.8 Non-affirmation

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

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

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

9.4.9 Affirmation

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

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

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

9.4.10 Routing

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

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

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

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

10 Security model

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

The security features are an optional extension to the MHS that can be used to minimize 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 1 – 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 standardization.

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

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

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.

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.