

**Implementation of
ISO/IEC 10021-2:1990**

**Information
technology —
Text Communication —
Message-Oriented Text
Interchange Systems
(MOTIS) —**

Part 2: Overall Architecture

UDC 681.3:621:39

Committees responsible for this British Standard

The preparation of this British Standard was entrusted by the Information Systems Technology Standards Policy Committee (IST/-) to Technical Committee IST/18, upon which the following bodies were represented:

- British Computer Society
- British Facsimile Industry Consultative Committee
- British Photographic Association
- British Printing Industries Federation
- British Telecommunications plc
- Computing Services Association
- Department of Trade and Industry (Information Technology Division)
- EEA (The Association of Electronics, Telecommunications and Business Equipment Industries)
- HM Treasury (Central Computer and Telecommunications Agency)
- Her Majesty's Stationery Office
- Joint Network Team
- Ministry of Defence
- National Computer Users' Forum
- National Computing Centre Ltd
- SGML Users' Group
- University of London
- User Standards Forum for Information Technology (Institute of Data Processing Management)

Amendments issued since publication

Amd. No.	Date	Comments
6847	September 1991	
7140	July 1992	
7272	August 1992	
7541	December 1992	
8170	May 1994	
8608	May 1995	
8386	January 1995	
8548	May 1995	Indicated by a sideline in the margin

This British Standard, having been prepared under the direction of the Information Systems Technology Standards Policy Committee, was published under the authority of the Standards Board and comes into effect on 29 March 1991

© BSI 05-2000

The following BSI references relate to the work on this standard:
Committee reference IST/18
Draft announced in *BSI News* November 1990

ISBN 0 580 19507 4

Contents

	Page
Committees responsible	Inside front cover
National foreword	ii
Foreword	ix
Text of ISO/IEC 10021-2	1

National foreword

This British Standard reproduces verbatim ISO/IEC 10021-2:1990 including Technical Corrigenda 1, 2, 3, 4, 5, 6 and 7 and Amendments 1 and 2 and implements it as the UK national standard.

This British Standard is published under the direction of the Information Systems Technology Standards Policy Committee whose Technical Committee IST/18 has the responsibility to:

- aid enquirers to understand the text;
- present to the responsible international committee any enquiries on interpretation, or proposals for change, and keep UK interests informed;
- monitor related international and European developments and promulgate them in the UK.

NOTE International and European Standards, as well as overseas standards, are available from BSI Sales Department, BSI, Linford Wood, Milton Keynes, MK14 6LE.

A British Standard does not purport to include all the necessary provisions of a contract. Users of British Standards are responsible for their correct application.

Compliance with a British Standard does not of itself confer immunity from legal obligations.

Summary of pages

This document comprises a front cover, an inside front cover, pages i and ii, the ISO/IEC title page, pages ii to x, pages 1 to 73 and a back cover.

This standard has been updated (see copyright date) and may have had amendments incorporated. This will be indicated in the amendment table on the inside front cover.

INTERNATIONAL STANDARD

ISO/IEC
10021-2

First edition
1990-12-01

AMENDMENT 2
1994-08-01

Information technology — Text Communication — Message-Oriented Text Interchange Systems (MOTIS) —

Part 2: Overall Architecture

AMENDMENT 2: Minor enhancements: Multinational organizations and terminal-form addresses

*Technologies de l'information — Communication de texte — Systèmes d'échange
de texte en mode message —*

Partie 2: Architecture générale

*AMENDEMENT 2: Améliorations mineures: Adresses d'organisations
multinationales et de fiches de terminaux*



Reference number
ISO/IEC 10021-2:1990/Amd.2:1994(E)

AVA Documents
Document Sharing Hub

Contents

	Page
Foreword	ix
Section 1. Introduction	
Introduction	1
1 Scope	1
2 Normative references	2
2.1 Open Systems Interconnection	2
2.2 Directory Systems	3
2.3 Message Handling Systems	3
2.4 Country Codes	3
2.5 Network Addresses	3
3 Definitions	4
3.1 Open Systems Interconnection	4
3.2 Directory Systems	5
3.3 Message Handling Systems	5
4 Abbreviations	5
5 Conventions	5
5.1 ASN.1	5
5.2 Grade	6
5.3 Terms	6
Section 2. Abstract Models	
6 Overview	7
7 Functional Model	7
7.1 Primary Functional Objects	7
7.1.1 The Message Handling System	8
7.1.2 Users	8
7.1.3 Distribution Lists	8
7.2 Secondary Functional Objects	8
7.2.1 The Message Transfer System	9
7.2.2 User Agents	9
7.2.3 Message Stores	9
7.2.4 Access Units	10
7.3 Tertiary Functional Objects	10
7.3.1 Message Transfer Agents	10
7.4 Selected AU Types	10
7.4.1 Physical Delivery	10
7.4.2 Telematic	11
7.4.3 Telex	11
8 Information Model	11
8.1 Messages	11
8.2 Probes	12
8.3 Reports	12
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	15
9.3.3 Import	16
9.3.4 Transfer	16
9.3.5 Export	16

		Page
9.3.6	Delivery	16
9.3.7	Retrieval	16
9.3.8	Receipt	16
9.4	Transmittal Events	17
9.4.1	Splitting	17
9.4.2	Joining	17
9.4.3	Name Resolution	17
9.4.4	DL Expansion	17
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	18
10	Security Model	19
10.1	Security Policies	19
10.2	Security Services	19
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	21
10.2.1.3	Proof of Delivery Security Service	21
10.2.2	Secure Access Management Security Service	21
10.2.2.1	Peer Entity Authentication Security Service	21
10.2.2.2	Security Context Security Service	21
10.2.3	Data Confidentiality Security Services	21
10.2.3.1	Connection Confidentiality Security Service	21
10.2.3.2	Content Confidentiality Security Service	22
10.2.3.3	Message Flow Confidentiality Security Service	22
10.2.4	Data Integrity Security Services	22
10.2.4.1	Connection Integrity Security Service	22
10.2.4.2	Content Integrity Security Service	22
10.2.4.3	Message Sequence Integrity Security Service	22
10.2.5	Non-Repudiation Security Services	23
10.2.5.1	Non-repudiation of Origin Security Service	23
10.2.5.2	Non-Repudiation of Submission Security Service	23
10.2.5.3	Non-Repudiation of Delivery Security Service	23
10.2.6	Message Security Labelling Security Service	23
10.2.7	Security Management Services	23
10.2.7.1	Change Credentials Security Service	23
10.2.7.2	Register Security Service	23
10.2.7.3	MS-Register Security Service	24
10.3	Security Elements	24
10.3.1	Authentication Security Elements	24
10.3.1.1	Authentication Exchange Security Element	24
10.3.1.2	Data Origin Authentication Security Elements	24
10.3.1.3	Proof of Submission Security Element	25
10.3.1.4	Proof of Delivery Security Element	25

	Page
10.3.2 Secure Access Management Security Elements	25
10.3.2.1 Security Context Security Element	25
10.3.2.2 Register Security Element	25
10.3.2.3 MS-Register Security Element	25
10.3.3 Data Confidentiality Security Elements	26
10.3.3.1 Content Confidentiality Security Element	26
10.3.3.2 Message Argument Confidentiality Security Element	26
10.3.4 Data Integrity Security Elements	26
10.3.4.1 Content Integrity Security Element	26
10.3.4.2 Message Argument Integrity Security Element	26
10.3.4.3 Message Sequence Integrity Security Element	26
10.3.5 Non-repudiation Security Elements	27
10.3.6 Security Label Security Elements	27
10.3.6.1 Message Security Label Security Element	27
10.3.7 Security Management Security Elements	27
10.3.7.1 Change Credentials Security Element	27
10.3.8 Double Enveloping Technique	27
10.3.9 Encoding for Encryption and Hashing	27
Section 3. Configurations	
11 Overview	28
12 Functional Configurations	28
12.1 Regarding the Directory	28
12.2 Regarding the Message Store	28
13 Physical Configurations	29
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	31
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	33
15 The Global MHS	33
Section 4. Naming, Addressing, and Routing	
16 Overview	34
17 Naming	34

		Page
17.1	Directory Names	34
17.2	O/R Names	34
18	Addressing	35
18.1	Attribute Lists	35
18.2	Character Sets	35
18.3	Standard Attributes	36
18.3.1	Administration-domain-name	36
18.3.2	Common-name	37
18.3.3	Country-name	37
18.3.4	Extension-postal-O/R-address-components	37
18.3.5	Extension-physical-delivery-address-components	37
18.3.6	Local-postal-attributes	37
18.3.7	Network-address	37
18.3.8	Numeric-user-identifier	38
18.3.9	Organization-name	38
18.3.10	Organizational-unit-names	38
18.3.11	Pds-name	38
18.3.12	Personal-name	38
18.3.13	Physical-delivery-country-name	38
18.3.14	Physical-delivery-office-name	38
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	39
18.3.19	Postal-code	39
18.3.20	Poste-restante-address	39
18.3.21	Private-domain-name	39
18.3.22	Street-address	39
18.3.23	Terminal-identifier	39
18.3.24	Terminal type	39
18.3.25	Unformatted-postal-address	40
18.3.26	Unique-postal-name	40
18.4	Attribute List Equivalence	40
18.5	O/R Address Forms	40
18.5.1	Mnemonic O/R Address	41
18.5.2	Numeric O/R Address	41
18.5.3	Postal O/R Address	42
18.5.4	Terminal O/R Address	42
18.5.5	Determination of Address Forms	42
18.6	Conditional Attributes	43
19	Routing	43
Section 5. Use of the Directory		
20	Overview	44
21	Authentication	44
22	Name Resolution	44
23	DL Expansion	44
24	Capability Assessment	44
Section 6. OSI Realization		
25	Overview	45

	Page
26	Application Service Elements
26.1	The ASE Concept
26.2	Symmetric and Asymmetric ASEs
26.3	Message Handling ASEs
26.3.1	Message Transfer
26.3.2	Message Submission
26.3.3	Message Delivery
26.3.4	Message Retrieval
26.3.5	Message Administration
26.4	Supporting ASEs
26.4.1	Remote Operations
26.4.2	Reliable Transfer
26.4.3	Association Control
27	Application Contexts
Annex A (normative) Directory Object Classes and Attributes	50
A.1	Object Classes
A.1.1	MHS Distribution List
A.1.2	MHS Message Store
A.1.3	MHS Message Transfer Agent
A.1.4	MHS User
A.1.5	MHS User Agent
A.2	Attributes
A.2.1	MHS Deliverable Content Length
A.2.2	MHS Deliverable Content Types
A.2.3	MHS Deliverable EITs
A.2.4	MHS DL Members
A.2.5	MHS DL Submit Permissions
A.2.6	MHS Message Store Directory Name
A.2.7	MHS O/R Addresses
A.2.8	MHS Supported Automatic Actions
A.2.9	MHS Supported Content Types
A.2.10	MHS Supported Optional Attributes
A.3	Attribute Syntaxes
A.3.1	MHS DL Submit Permission
A.3.2	MHS O/R Address
A.3.3	MHS O/R Name
Annex B (normative) Reference Definition of Object Identifiers	54
Annex C (normative) Reference Definition of Directory Object Classes and Attributes	55
Annex D (informative) Security Threats	58
D.1	Masquerade
D.2	Message Sequencing
D.3	Modification of Information
D.4	Denial of Service
D.5	Repudiation
D.6	Leakage of Information
D.7	Other Threats

	Page
Annex E (normative) Provision of Security Services in ISO/IEC 10021-4	61
Annex F (informative) Representation of O/R Addresses for Human Usage	62
F.1 Purpose	62
F.2 Scope	62
F.3 Format	62
F.3.1 General	62
F.3.2 Labelled format	62
F.3.2.1 Syntax	62
F.3.2.2 Terminal-type	64
F.3.2.3 Domain-defined attribute	64
F.3.3 Self-explanatory format	64
F.4 User Interface	65
Annex G (informative) Use of O/R Addresses by Multinational Organization	66
G.1 Addressing principles	66
G.2 Example configurations	67
G.2.1 Multiple Independent PRMDs	67
G.2.2 A single PRMD, named from a “home” country	68
G.2.3 A single PRMD with multiple country and domain names	68
G.3 Alias O/R addresses	69
Annex H (informative) Differences Between ISO/IEC 10021-2 and CCITT Recommendation X.402	70
Annex I (informative) Index	71
Figure 1 — The Message Handling Environment	8
Figure 2 — The Message Handling System	9
Figure 3 — The Message Transfer System	10
Figure 4 — A Message’s Envelope and Content	12
Figure 5 — The Information Flow of Transmittal	14
Figure 6 — Simplified MHS Functional Model	20
Figure 7 — Functional Configurations Regarding the MS	28
Figure 8 — Messaging System Types	29
Figure 9 — Representative Physical Configurations	31
Figure 10 — Representative Organizational Configurations	32
Figure 11 — The Global MHS	33
Figure 12 — The ASE Concept	45
Figure 13 — Symmetric and Asymmetric ASEs	46
Figure 14 — Terminology for Asymmetric ASEs	47
Figure 15 — Multiple Asymmetric ASEs	47
Figure G.1 — Multiple Independent PRMDs	67
Figure G.2 — A single PRMD with a single name	68
Figure G.3 — A single PRMD with multiple country and domain names	68
Table 1 — Specifications for Message Handling Systems	1
Table 2 — Specifications for Directories	2
Table 3 — Specifications for MHS Foundations	2
Table 4 — Conveyable Information Objects	11
Table 5 — Transmittal Steps	15
Table 6 — Transmittal Events	17
Table 7 — Message Transfer Security Services	20

	Page
Table 8 — Messaging Systems	29
Table 9 — Standard Attributes	36
Table 10 — Forms of O/R Address	41
Table 11 — Message Handling ASEs	48
Table 12 — Supporting ASEs	48
Table D.1 — Use of MHS Security Services	59
Table E.1 — MHS Security Service Provision	61
Table F.1 — Standard Attributes of the Mnemonic Address Form	63
Table F.2 — Physical Delivery Attributes	63
Table F.3 — Other Attributes	64

Descriptors: Data processing, information interchange, network interconnection, open systems interconnection, data transmission, text communication, messages, architecture.

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. 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.

Amendment 2 to International Standard ISO/IEC 10021-2:1990 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee 18, *Document processing and related communication*.

Section 1. Introduction

Introduction

This part of ISO/IEC 10021 is one of a number of parts of ISO/IEC 10021 [the International Standards for Message-Oriented Text Interchange Systems (MOTIS)]. ISO/IEC 10021 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 part of ISO/IEC 10021 specifies the overall architecture of the MHS and serves as a technical introduction to it.

The text of this part of ISO/IEC 10021 is the subject of joint CCITT-ISO agreement. The corresponding CCITT specification is Recommendation X.402.

1 Scope

This part of ISO/IEC 10021 defines the overall architecture of the MHS and serves as a technical introduction to it.

Other aspects of Message Handling are specified in other parts of ISO/IEC 10021. A non-technical overview of Message Handling is provided by ISO/IEC 10021-1. The conventions used in the definition of the abstract services provided by MHS components are defined in ISO/IEC 10021-3. The abstract service the MTS provides and the procedures that govern its distributed operation are defined in ISO/IEC 10021-4. The abstract service the MS provides is defined in ISO/IEC 10021-5. The application protocols that govern the interactions of MHS components are specified in ISO/IEC 10021-6. The Interpersonal Messaging System, an application of Message Handling, is defined in ISO/IEC 10021-7.

The ISO International Standards and CCITT Recommendations on Message Handling are summarized in Table 1.

Table 1 — Specifications for Message Handling Systems

ISO/IEC	CCITT	SUBJECT MATTER
Introduction		
10021-1	X.400	Service and system overview
10021-2	X.402	Overall architecture
Various Aspects		
-	X.403	Conformance testing
10021-3	X.407	Abstract service definition conventions
-	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

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

Table 2 — Specifications for Directories

ISO/IEC	CCITT	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

The architectural foundation for Message Handling is provided by other International Standards. The OSI Reference Model is defined in 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 ISO 8824 and ISO 8825. The means for establishing and releasing associations, the ACSE, is defined in ISO 8649 and ISO 8650. The means for reliably conveying APDUs over associations, the RTSE, is defined in ISO/IEC 9066. The means for making requests of other open systems, the ROSE, is defined in ISO/IEC 9072.

The ISO International Standards and CCITT Recommendations which form the foundation for Message Handling are summarized in Table 3.

Table 3 — Specifications for MHS Foundations

ISO	CCITT	SUBJECT MATTER
Model		
7498	X.200	OSI Reference Model
ASN.1		
8824	X.208	Abstract syntax notation
8825	X.209	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		
9072-1	X.219	Service definition
9072-2	X.229	Protocol specification

This part of ISO/IEC 10021 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. Annexes provide important supplemental information.

No requirements for conformance to this part of ISO/IEC 10021 are imposed.

2 Normative references

The following standards contain provisions which, through reference in this text, constitute provisions of this part of ISO/IEC 10021. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this part of ISO/IEC 10021 are encouraged to investigate the possibility of applying the most recent editions of the standards listed below. Members of ISO and IEC maintain registers of currently valid International Standards.

2.1 Open Systems Interconnection

This part of ISO/IEC 10021 and others in the set cite the following OSI specifications:

ISO 7498:1984, *Information processing systems — Open Systems Interconnection — Basic Reference Model*.

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

ISO 8649:1988, *Information processing systems — Open Systems Interconnection — Service definition for the Association Control Service Element.*

ISO 8650:1988, *Information processing systems — Open Systems Interconnection — Protocol specification for the Association Control Service Element.*

ISO 8822:1988, *Information processing systems — Open Systems Interconnection — Connection oriented presentation service definition.*

ISO 8824:1990, *Information processing systems — Open Systems Interconnection — Specification of Abstract Syntax Notation One (ASN.1).*

ISO 8825:1990, *Information processing systems — Open Systems Interconnection — Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1).*

ISO/IEC 9066:1989, *Information processing systems — Text communication — Reliable Transfer — Part 1: Model and service definition — Part 2: Protocol specification.*

ISO/IEC 9072:1989, *Information processing systems — Text communication — Remote operations — Part 1: Model, notation and service definition — Part 2: Protocol specification.*

2.2 Directory Systems

This part of ISO/IEC 10021 and others in the set cite the following Directory System specifications:

ISO/IEC 9594:1990, *Information technology — Open Systems Interconnection — The Directory*

- *Part 1: Overview of concepts, models, and services;*
- *Part 2: Models;*
- *Part 3: Abstract service definition;*
- *Part 4: Procedures for distributed operation;*
- *Part 5: Protocol specifications;*
- *Part 6: Selected attribute types;*
- *Part 7: Selected object classes;*
- *Part 8: Authentication framework.*

2.3 Message Handling Systems

This part of ISO/IEC 10021 and others in the set cite the following Message Handling System specifications:

ISO/IEC 10021:1990, *Information technology — Text communication — Message-Oriented Text Interchange Systems (MOTIS)*

- *Part 1: Service and system overview;*
- *Part 3: Abstract service definition conventions;*
- *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.*

CCITT T.330:1988, *Telematic access to IPMS.*

CCITT X.403:1988, *Message handling systems: Conformance testing.*

CCITT X.408:1988, *Message handling systems: Encoded information type conversion rules.*

2.4 Country Codes

This part of ISO/IEC 10021 cites the following Country Code specifications:

ISO 3166:1988, *Codes for the representation of names of countries.*

CCITT X.121:1988, *International numbering plan for public data networks.*

2.5 Network Addresses

This part of ISO/IEC 10021 cites the following Network Address specifications:

CCITT Recommendation E.163 (1988), *Numbering plan for the international telephone services.*

CCITT Recommendation E.164 (1988), *Numbering plan for the ISDN era.*

3 Definitions

For the purposes of this part of ISO/IEC 10021 and others in the set, the following definitions apply.

3.1

Open Systems Interconnection

This part of ISO/IEC 10021 and others in the set make use of the following terms defined in ISO 7498, 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).

This part of ISO/IEC 10021 and others in the set make use of the following terms defined in ISO 8824 and ISO 8825, 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) macro;
- h) module;
- i) tag;
- j) type; and
- k) value.

This part of ISO/IEC 10021 and others in the set make use of the following terms defined in ISO 8649:

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

This part of ISO/IEC 10021 and others in the set make use of the following terms defined in ISO/IEC 9066-1:

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

This part of ISO/IEC 10021 and others in the set make use of the following terms defined in ISO/IEC 9072-1:

- 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 part of ISO/IEC 10021 and others in the set make use of the following terms defined in 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 part of ISO/IEC 10021 the terms indexed in Annex G apply.

4 Abbreviations

For the purposes of this part of ISO/IEC 10021 the abbreviations indexed in Annex G apply.

5 Conventions

This part of ISO/IEC 10021 uses the descriptive conventions identified below.

5.1 ASN.1

This part of ISO/IEC 10021 uses several ASN.1-based descriptive conventions in Annex A and Annex C to define the Message Handling-specific information the Directory may hold. In particular, it uses the OBJECT-CLASS, ATTRIBUTE, and ATTRIBUTE-SYNTAX macros of ISO/IEC 9594-2 to define Message Handling-specific object classes, attributes, and attribute syntaxes.

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 part of ISO/IEC 10021 describes a class of data structure (e.g., O/R 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 part of ISO/IEC 10021, applies.
- d) **conditional (C)**: A conditional component shall be present in an instance of the class as dictated by this part of ISO/IEC 10021.

5.3 Terms

Throughout the remainder of this part of ISO/IEC 10021, 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 parts of ISO/IEC 10021.

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 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 parts of ISO/IEC 10021.

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 ISO/IEC 10021-7 and CCITT 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 ISO/IEC 10021. 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.

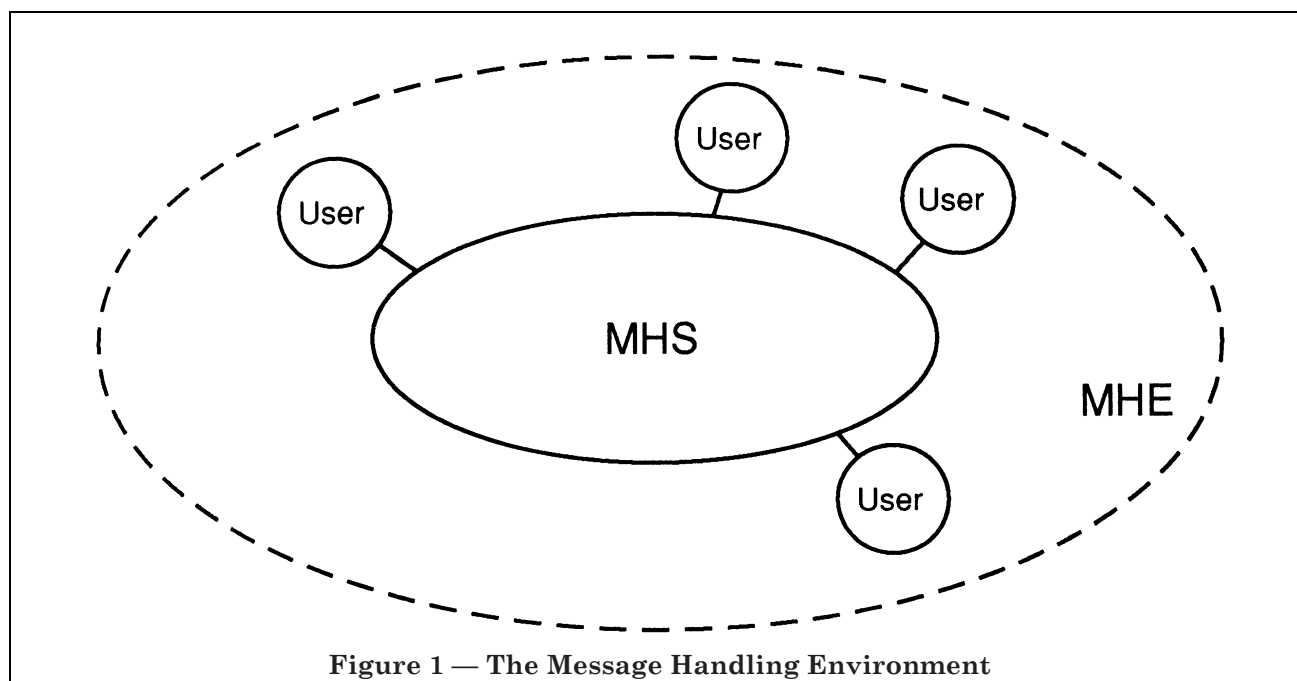


Figure 1 — The Message Handling Environment

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.

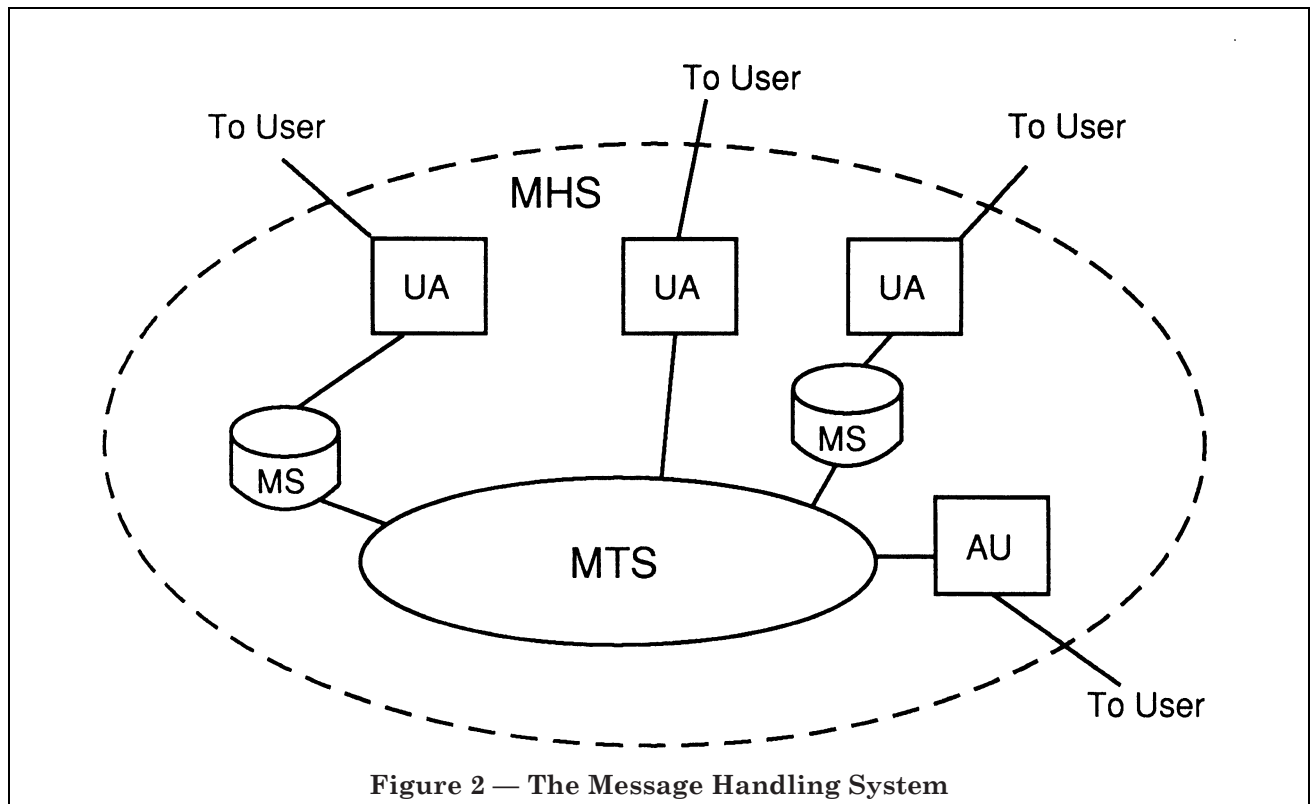


Figure 2 — The Message Handling System

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 a number of UAs.

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

7.2.3 Message Stores

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

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

The MHS comprises any number of MSs.

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

7.2.4 Access Units

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

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

The MHS comprises any number of AUs.

7.3 Tertiary Functional Objects

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

The situation is depicted in Figure 3.

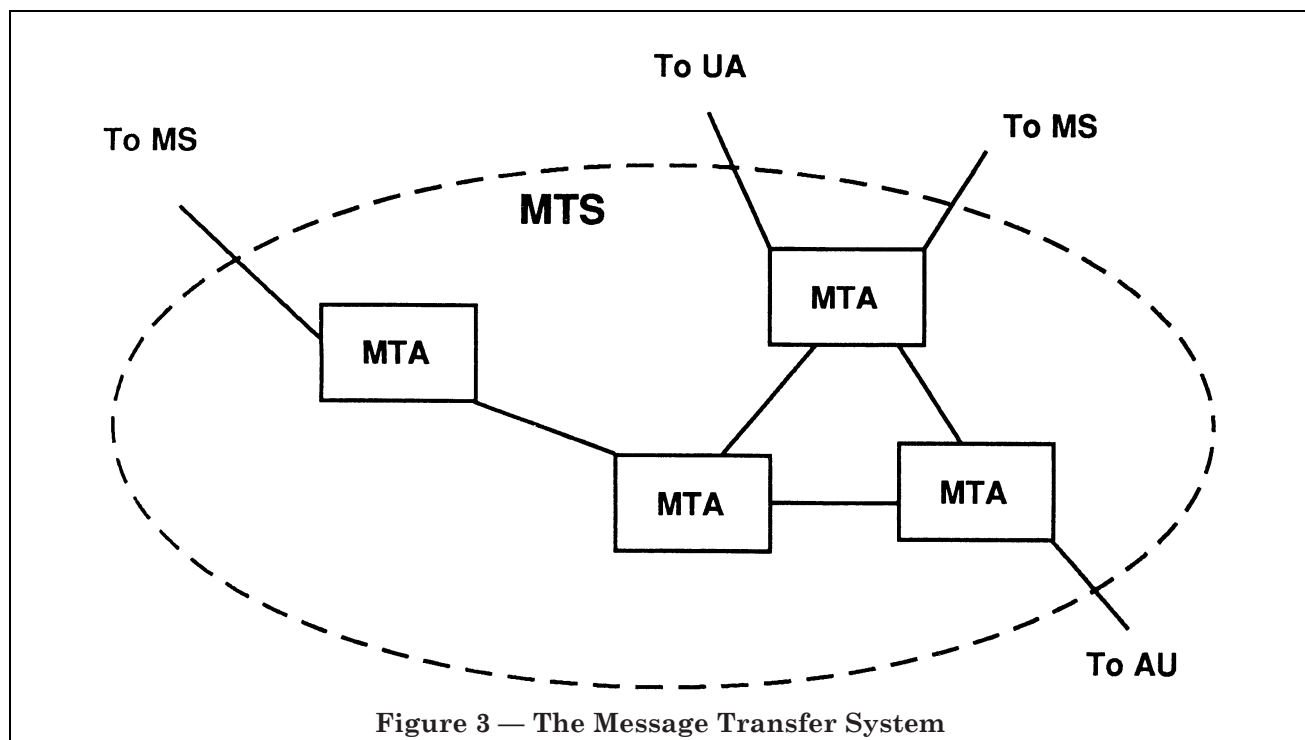


Figure 3 — The Message Transfer System

7.3.1 Message Transfer Agents

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

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

The MTS comprises any number of MTAs.

7.4 Selected AU Types

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

7.4.1 Physical Delivery

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

The transformation of a *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*.

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 ISO/IEC 10021-7).

7.4.2 Telematic

Telematic access units, which support Interpersonal Messaging exclusively, are introduced in ISO/IEC 10021-7.

7.4.3 Telex

Telex access units, which support Interpersonal Messaging exclusively, are introduced in 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 parts of ISO/IEC 10021.

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

Table 4 — Conveyable Information Objects

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

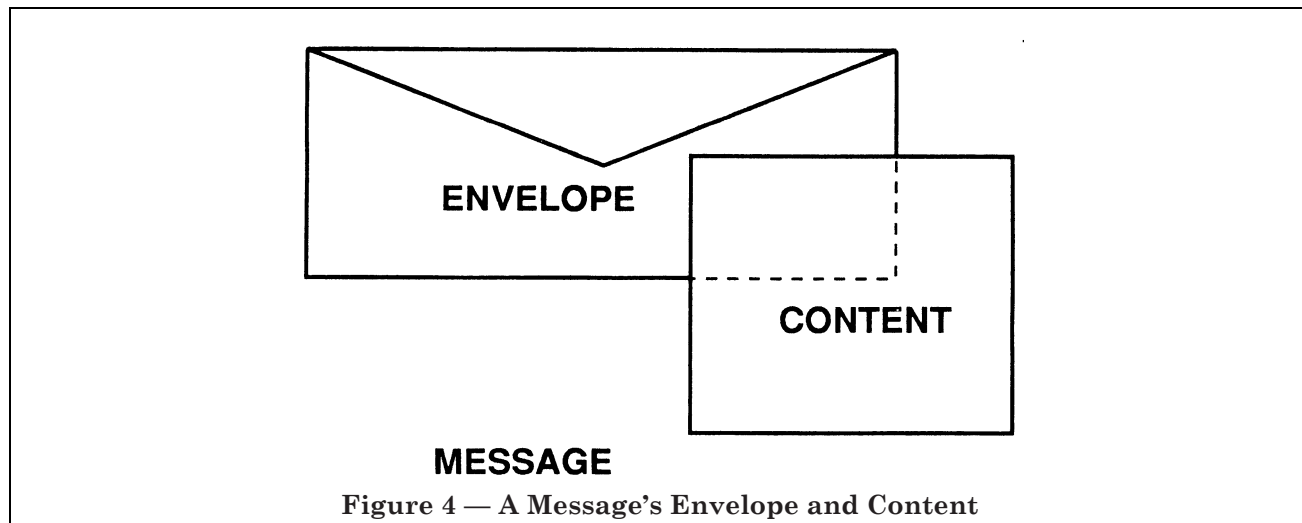
Legend	
S	ultimate source
D	ultimate destination

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

8.1 Messages

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

- 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.



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

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

8.2 Probes

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

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

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

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

8.3 Reports

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

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

A report concerning a particular *potential recipient* is conveyed to the *originator* of the subject message or probe unless the *potential recipient* is a *member recipient*. In the latter case, the report is conveyed to the DL of which the *member recipient* is a member. As a local matter (i.e., by policy established for that particular DL), the report may be further conveyed to the DL's owner; either to another, 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 parts of ISO/IEC 10021.

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. 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*.

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.