INTERNATIONAL TELECOMMUNICATION UNION

CCITT

THE INTERNATIONAL
TELEGRAPH AND TELEPHONE
CONSULTATIVE COMMITTEE

X.402

(11/1988)

SERIES X: DATA COMMUNICATION NETWORKS:
MESSAGE HANDLING SYSTEMS

MESSAGE HANDLING SYSTEMS: OVERALL ARCHITECTURE

Reedition of CCITT Recommendation X.402 published in the Blue Book, Fascicle VIII.7 (1988)

NOTES

1 CCITT Recommendation X.402 was published in Fascicle VIII.7 of the *Blue Book*. This file is an extract from the *Blue Book*. While the presentation and layout of the text might be slightly different from the *Blue Book* version, the contents of the file are identical to the *Blue Book* version and copyright conditions remain unchanged (see below).

2 In this Recommendation, the expression “Administration” is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

© ITU 1988, 2008

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

Recommendation X.402

MESSAGE HANDLING SYSTEMS: OVERALL ARCHITECTURE[1]

(Melbourne, 1988)

The establishment in various countries of telematic services and computer-based store-and-forward message services in association with public data networks creates a need to produce standards to facilitate international message exchange between subscribers to such services.

The CCITT,

considering

(a) the need for Message Handling Systems;

(b) the need to transfer and store messages of different types;

(c) that Recommendation X.200 defines the Reference Model of Open Systems Interconnection for CCITT applications;

(d) that Recommendations X.208, X.217, X.218 and X.219 provide the foundation for CCITT applications;

(e) that the X.500-series Recommendations define Directory Systems;

(f) that Message Handling Systems are defined in a series of Recommendations: X.400, X.402, X.403, X.407, X.408, X.411, X.413, and X.419;

(g) that Interpersonal Messaging is defined in Recommendations X.420 and T.330,

unanimously declares

(1) that the abstract models of a Message Handling System are defined in § 2;

(2) that the configurations of a Message Handling System are defined in § 3;

(3) that naming, addressing, and routing within Message Handling Systems are defined in § 4;

(4) that the use of the Directory by Message Handling Systems is defined in § 5;

(5) that the OSI realization of a Message Handling System is specified in § 6.

TABLE OF CONTENTS

[1] Recommendation X.402 and ISO 10021—2 [Information Processing Systems — Text Communications — MOTIS — Overall Architecture] were developed in close collaboration and are technically aligned, except for the differences noted in Annex F.

SECTION 2 – *Abstract models*

SECTION 3 – *Configurations*

SECTION 1 – INTRODUCTION

0 Introduction

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

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

The Recommendation specifies the overall architecture of the MHS and serves as a technical introduction to it.

The text of this Recommendation is the subject of joint CCITT-ISO agreement. The corresponding ISO specification is ISO 10021-2.

1 Scope

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

Other aspects of Message Handling are specified in other Recommendations. A non-technical overview of Message Handling is provided by Recommendation X.400. The conformance testing of MHS components is described in Recommendation X.403. The conventions used in the definition of the abstract services provided by MHS components are defined in Recommendation X.407. The detailed rules by which the MTS converts the contents of messages from one EIT to another are defied in Recommendation X.408. The abstract service the MTS provides and the procedures that govern its distributed operation are defined in Recommendation X.411. The abstract service the MS provides is defined in Recommendation X.413. The application protocols that govern the interactions of MHS components are specified in Recommendation X.419. The Interpersonal Messaging System, an application of MHS Handling, is defined in Recommendation X.420. Telematic access to the Interpersonal Messaging System is specified in Recommendation T.330.

The CCITT Recommendations and ISO International Standards of Message Handling are summarized in Table 1/X.402.

TABLE 1/X.402

Specifications for message handling systems

CCITT	ISO	Subject matter
Introduction		
X.400 X.402	8505-1 8505-2	Service and system overview Overall architecture
Various aspects		
X.403 X.407 X.408	– 8883-2 –	Conformance testing Abstract service definition conventions Encoded information type conversion rules
Abstract services		
X.411 X.413	8883-1 TBS-1	MTS abstract service definition and procedures for distributed operation MS abstract service definition
Protocols		
X.419	8505-2	Protocol specifications
Interpersonal messaging system		
X.420 T.330	9065 –	Interpersonal messaging system Telematic access to IPMS

The Directory, the principal means for disseminating communication-related information among MHS components, is defined in the X.500-series Recommendations (see Table 2/X.402).

The architectural foundation for Message Handling is provided by other Recommendations. The OSI Reference Model is defined in Recommendation X.200. The notation for specifying the data structures of abstract services and application protocols, ASN.1, and the associated encoding rules are defined in Recommendations X.208 and X.209. The means for establishing and releasing associations, the ACSE, is defined in Recommendations X.217 and X.227. The means for reliably conveying APDUs over associations, the RTSE, is defined by Recommendations X.218 and X.228. The means for making requests of other open systems, the ROSE, is defined in Recommendations X.219 and X.229.

The CCITT Recommendations and ISO International Standards basic to Message Handling are summarized in Table 3/X.402.

TABLE 2/X.402

Specifications for directories

CCITT	ISO	Subject matter
Model		
X.200	7498	OSI reference model
X.500	9594-1	Overview
X.501	9594-2	Models
X.509	9594-8	Authentication framework
X.511	9594-3	Abstract service definition
X.518	9594-4	Procedures for distributed operation
X.519	9594-5	Protocol specifications
X.520	9594-6	Selected attribute types
X.521	9594-7	Selected object classes

TABLE 3/X.402

Specifications for MHS foundations

CCITT	ISO	Subject matter
Model		
X.200	7498	OSI reference model
ASN.1		
X.208 X.209	8824 8825	Abstract syntax notation Basic encoding rules
Association control		
X.217 X.227	8649 8650	Service definition Protocol specification
Reliable transfer		
X.218 X.228	9066-1 9066-2	Service definition Protocol specification
Remote operations		
X.219 X.229	9072-1 9072-2	Service definition Protocol specification

This Recommendation is structured as follows. Section 1 is this introduction. 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 Recommendation are imposed.

2 References

This Recommendation and others in the set cite the documents below.

2.1 *Open systems interconnection*

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

X.200 Reference model of open systems interconnection for CCITT applications (see also ISO 7498)

X.208 Specification of abstract syntax notation one (ASN.1) (see also ISO 8824)

X.209 Specification of basic encoding rules for abstract syntax notation (see also ISO 8825)

X.217 Association control service definition for open systems interconnection for CCITT applications (see also ISO 8649)

X.218 Reliable transfer: Model and service definition (see also ISO 9066-1)

X.219 Remote operations: Model, notation and service definition (see also ISO 9072-1)

X.227 Association control: Protocol specification for open systems interconnection for CCITT applications (see also ISO 8650)

X.228 Reliable transfer: Protocol specification (see also ISO 9066-2)

X.229 Remote operations: Protocol specification (see also ISO 9072-2)

2.2 *Directory systems*

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

X.500 The directory - Overview of concepts, models, and services (see also ISO 9594-1)

X.501 The directory - Models (see also ISO 9594-2)

X.509 The directory - Authentication framework (see also ISO 9594-8)

X.511 The directory - Abstract service definition (see also ISO 9594-3)

X.518 The directory - Procedures for distributed operation (see also ISO 9594-4)

X.519 The directory - Protocol specifications (see also ISO 9594-5)

X.520 The directory - Selected attribute types (see also ISO 9594-6)

X.521 The directory - Selected object classes (see also ISO 9594-7)

2.3 *Message handling systems*

This Recommendation and others in the set cite the following message handling system specifications:

T.330 Telematic access to interpersonal messaging system

X.400 Message handling: System and service overview (see also ISO 10021-1)

X.403 Message handling systems: Conformance testing

X.407 Message handling systems: Abstract service definition conventions (see also ISO 10021-3)

X.408 Message handling systems: Encoded information type conversion rules

X.411 Message handling systems: Message transfer system: Abstract service definition and procedures (see also ISO 10021-4)

X.413 Message handling systems: Message store: Abstract service definition (see also ISO 10021-5)

X.419 Message handling systems: Protocol specifications (see also ISO 10021-6)

X.420 Message handling systems: Interpersonal messaging system (see also ISO 10021-7)

3 **Definitions**

For the purposes of this Recommendation and others in the set, the definitions below apply.

3.1 *Open systems interconnection*

3.1.1 This Recommendation and others in the set use the following terms defined in Recommendation X.200, 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;

o) user element (UE).

3.1.2 This Recommendation and others in the set use the following terms defined in Recommendations X.208 and X.209, 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.

3.1.3 This Recommendation and others in the set use the following terms defined in Recommendation X.217:

- a) application association; association;
- b) application context (AC);
- c) association control service element (ACSE);
- d) initiator;
- e) responder.

3.1.4 This Recommendation and others in the set use the following terms defined in Recommendation X.218:

- a) Reliable transfer (RT); and
- b) Reliable transfer service element (RTSE).

3.1.5 This Recommendation and others in the set use the following terms defined in Recommendation X.219:

- 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 Recommendation and others in the set use the following terms defined in the X.500-series Recommendations:

- 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;

m) strong authentication.

3.3 *Message handling systems*

For the purposes of this Recommendation and others in the set, the definitions indexed in Annex G apply.

4 Abbreviations

For the purposes of this Recommendation and others in the set, the abbreviations indexed in Annex G apply.

5 Conventions

This Recommendation uses the descriptive conventions identified below.

5.1 *ASN.1*

This Recommendation uses several ASN.1-based descriptive conventions in Annexes A and 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 Recommendation X.501 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.

Note that 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 Recommendation 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 Recommendation, applies.

d) **conditional (C)**: a conditional component shall be present in an instance of the class as dictated by this Recommendation.

5.3 *Terms*

Throughout the remainder of this Recommendation, 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.

6 Overview

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

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 Recommendation X.420.

7 Functional model

This clause provides a functional model of Message Handling. The concrete realization of the model is the subject of other Recommendations in the set.

The **Message Handling Environment**; 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 Recommendations X.420 and 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 Recommendation or others in the set. 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/X.402.

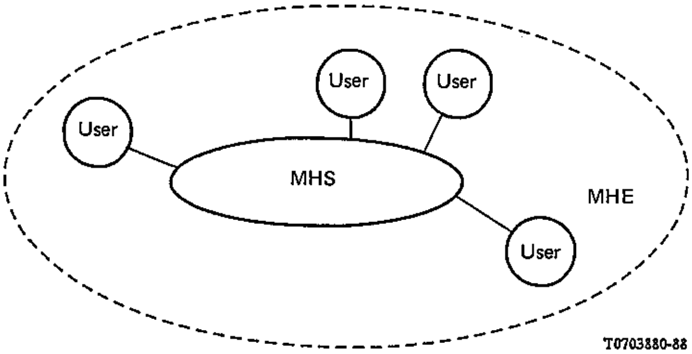


FIGURE 1/X.402

Message handling environment

7.1.1 *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**.

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/X.402.

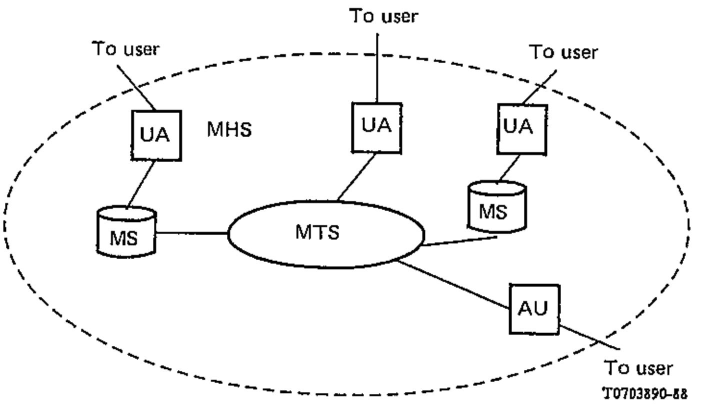


FIGURE 2/X.402

Message handling system

7.2.1 *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/X.402.

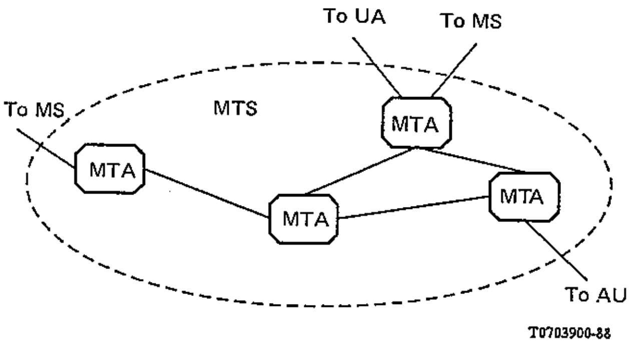


FIGURE 3/X.402

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 clauses 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 Recommendation X.420).

7.4.2 *Telematic*

Telematic access units, which support Interpersonal Messaging exclusively, are introduced in Recommendation X.420.

7.4.3 *Telex*

Telex access units, which support Interpersonal Messaging exclusively, are introduced in Recommendation X.420.

8 Information model

This clause provides an information model of Message Handling. The concrete realization of the model is the subject of other Recommendations in the set.

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/X.402. 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/X.402

Conveyable information objects

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

S Ultimate source

D Ultimate destination

The information objects, summarized in Table 4/X.402, are individually defined and described 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/X.402:

a) **envelope**: An information object whose composition varies from one *transmittal step* to another and that variously identifies the message's *originator* and *potential recipients*, documents its previous conveyance and directs its subsequent conveyance by the MTS, and characterizes its *content*.

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

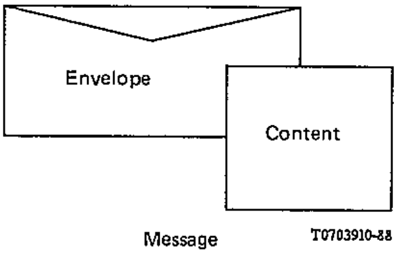


FIGURE 4/X.402

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 (an ASN.1 Object Identifier or Integer) 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 behavior 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 Recommendations in the set.

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/X.402. 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.

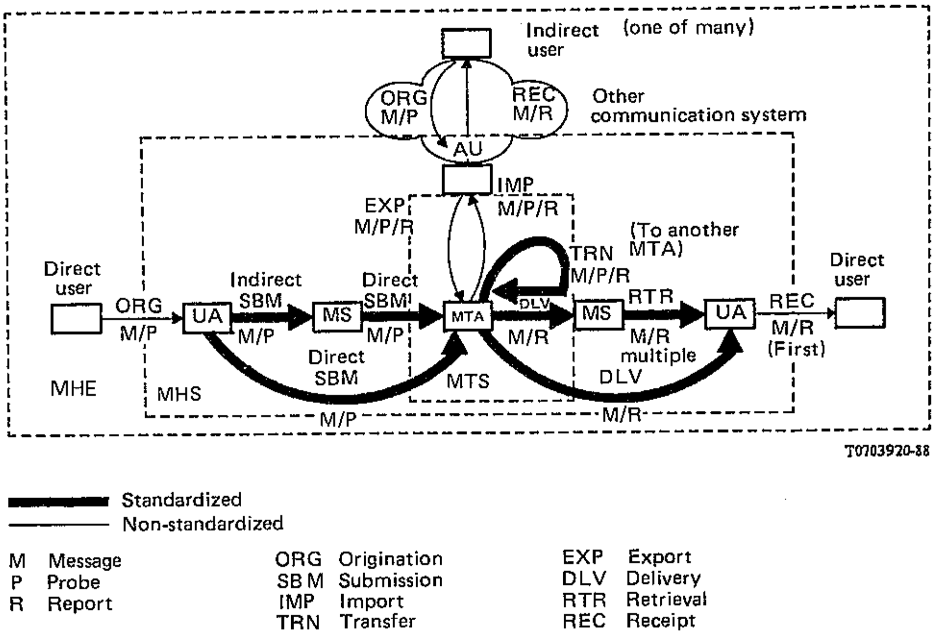


FIGURE 5/X.402

The Information flow of transmittal

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.

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.

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

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

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

a) **intended recipient**: One of the users and DLs the originator specifies as a message's or probe's intended destinations.

b) **originator-specified alternate recipient**: The user or DL (if any) to which the originator requests that a message or probe be conveyed if it cannot be conveyed to a particular intended recipient.

c) **member recipient**: A user or DL to which a message (but not a probe) is conveyed as a result of DL expansion.

d) **recipient-assigned alternate recipient**: The user or DL (if any) to which an intended, originator-specified alternate, or member recipient may have elected to redirect messages.

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

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

b) **actual recipient** (or **recipient**): A potential recipient for which delivery or affirmation takes place.

9.3 *Transmittal steps*

The kinds of steps that may occur in a transmittal are listed in the first column of Table 5/X.402. For each listed kind, the second column indicates whether this Recommendation and others in the set standardize such steps, the third column the kinds of information objects - messages, probes, and reports - that may be conveyed in such a step, the fourth column the kinds of functional objects - users, UAs, MSs, MTAs, and AUs - that may participate in such a step as the object's source or destination.

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

The kinds of transmittal steps, summarized in Table 5/X.402, are individually defined and described below.

TABLE 5/X.402

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	X	—	—	—	D	S
Transfer	Yes	X	X	X	—	—	—	SD	—
Export	No	X	X	X	—	—	—	S	D
Delivery	Yes	X	—	X	—	D	D	S	—
Retrieval	Yes	X	—	X	—	D	S	—	—
Reception	No	X	—	X	D	S	—	—	—

M	Message	S	Source
P	Probe	D	Destination
R	Report	X	Permitted

9.3.1 *Origination*

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

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

9.3.2 *Submission*

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

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

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

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

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

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

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

9.3.3 *Import*

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

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

9.3.4 *Transfer*

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

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

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

a) **internal transfer**: A transfer involving MTAs within a single MD.

b) **external transfer**: A transfer involving MTAs in different MDs.

9.3.5 *Export*

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

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

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/X.402. For each listed kind, the second column indicates the kinds of information objects - messages, probes, and reports - for which such events may be staged, the third column the kinds of functional objects - users, UAs, MSs, MTAs, and AUs - that may stage such events.

All the events occur within the MTS.

TABLE 6/X.402

Transmittal events

	Functional objets			Functional objects				
Transmittal event	M	P	R	User	UA	MS	MTA	AU
Splitting	X	X	—	—	—	—	X	—
Joining	X	X	X	—	—	—	X	—
Name resolution	X	X	—	—	—	—	X	—
DL expansion	X	—	—	—	—	—	X	—
Redirection	X	X	—	—	—	—	X	—
Conversion	X	X	—	—	—	—	X	—
Non-delivery	X	—	X	—	—	—	X	—
Non-affirmation	—	X	—	—	—	—	X	—
Affirmation	—	X	—	—	—	—	X	—
Routing	X	X	X	—	—	—	X	—

M	Message
P	Probe
R	Report
X	Permitted

The kinds of transmittal events, summarized in Table 6/X.402, are individually defined and described below.

9.4.1 *Splitting*

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

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

9.4.2 *Joining*

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

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

9.4.3 *Name resolution*

In a **name resolution** event, an MTA adds the corresponding *O/R address* to the *O/R 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 resolves a DL among a message's (but not a probe's) immediate recipients to its members which are thereby made member recipients. This event removes indirection from the immediate recipients' specification.

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 *O/R 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, and 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 Recommendations in the set. The security model provides a framework for describing the security services that counter potential threats (see Annex D) to the MTS and the security elements that support those services.

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

Note – Despite these security features, certain attacks may by be mounted against communication between a user and the MHS or against user-to-user communication (e.g. in the case of users accessing their UAs). To counter these attacks requires extensions to the present security model and services which are for further study.

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 Recommendation X.411. 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 Recommenda-tion X.411. 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 Recommendation X.411.

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 Recommendation. A future version of this Recommendation may make use of alternative mechanisms based on symmetric encipherment.

Note – The use of the terms "security service" and "security element" in this clause are not to be confused with the terms "service" and "element of service" as used in Recommendation X.400. 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 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/X.402.

Throughout the security service definitions that follow, reference is made to Figure 6/X.402, 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 D*ata Origin Authentication security services*

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

10.2.1.1.1 *Message Origin Authentication security service*

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

This security service can be provided using either the Message Origin Authentication or the Message Argument Integrity security element. The former can be used to provide the security service to any of the parties concerned (1-5 inclusive in Figure 6/X.402), whereas the latter can only be used to provide the security service to MTS-users (1 or 5 in Figure 6/X.402). The security element chosen depends on the prevailing security policy.

10.2.1.1.2 *Probe Origin Authentication security service*

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

This security service can be provided by using the Probe Origin Authentication security element. This security element can be used to provide the security service to any of the MTAs through which the probe is transferred (2-4 inclusive in Figure 6/X.402).

10.2.1.1.3 *Report Origin Authentication security service*

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

This security service can be provided by using the Report Origin Authentication security element. This security element can be used to provide the security service to the originator of the subject message or probe, as well as to any MTA through which the report is transferred (1-5 inclusive in Figure 6/X.402).

TABLE 7/X.402

Message transfer security services

	Service							
	UA/ UA	MS/ MTA	MTA / MS	MTA / UA	UA/ MS	UA/ MTA	MTA/ MTA	MS/ UA
Origin authentication								
Message origin authentication	*	*	—	*	—	—	—	—
Probe origin authentication	—	—	*	*	—	—	—	—
Report origin authentication	—	—	—	—	*	*	*	—
Proof of submission	—	—	—	—	—	—	*	—
Proof of delivery	*	—	—	—	—	—	—	a)
Secure access management								
Peer entity authentication	—	*	*	*	*	*	*	*
Security context	—	*	*	*	*	*	*	*
Data confidentiality								
Connection confidentiality	—	*	*	*	*	*	*	*
Connection confidentiality	*	—	—	—	—	—	—	—
Message flow confidentiality	*	—	—	—	—	—	—	—
Data integrity services								
Connection integrity	—	*	*	*	*	*	*	*
Content integrity	*	—	—	—	—	—	—	—
Message sequence integrity	*	—	—	—	—	—	—	—
Non-repudiation								
Non-repudiation of origin	*	—	—	*	—	—	—	—
Non-repudiation of submission	—	—	—	—	—	—	*	—
Non-repudation of delivery	*	—	—	—	—	—	—	—
Message security labelling								
Message security labelling	*	*	*	*	*	*	*	*
Security management service								
Change credentials	—	*	—	*	*	*	*	—
Register	—	*	—	*	—	—	—	—
MS-register	—	*	—	—	—	—	—	—

* 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*.

[a] This service is provided by the recipient's MS to the originator's UA.

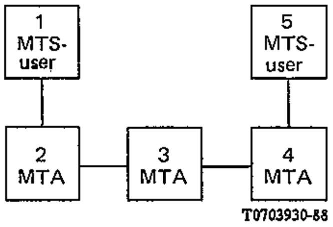


FIGURE 6/X.402

Simplified MHS functional model

10.2.1.2 *Proof of Submission security service*

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

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

10.2.1.3 *Proof of Delivery security service*

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

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

10.2.2 *Secure Access Management security service*

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

10.2.2.1 *Peer Entity Authentication security service*

This security service is provided for use at the establishment of a connection to confirm the identity of the connecting entity. It may be used on the links 1-2, 2-3, 3-4, or 4-5 in Figure 6/X.402 and provides confidence, at the time of usage only, that an entity is not attempting a masquerade or an unauthorised replay of a previous connection.

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

10.2.2.2 *Security Context security service*

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

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

10.2.3 *Data Confidentiality security services*

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

10.2.3.1 *Connection Confidentiality security service*

The MHS does not provide a Connection Confidentiality security service. However, data for the invocation of such a security service in underlying layers may be provided as a result of using the Authentication Exchange security element to provide the Peer Entity Authentication security service. The security service may be required on any of links 1-2, 2-3, 3-4, or 4-5 in Figure 6/X.402.

10.2.3.2 *Content Confidentiality security service*

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

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

10.2.3.3 *Message Flow Confidentiality security service*

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

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

10.2.4 *Data Integrity security services*

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

10.2.4.1 *Connection Integrity security service*

The MHS does not provide a Connection Integrity security service. However, data for the invocation of such a security service in underlying layers may be provided by using the Authentication Exchange security element to provide the Peer Entity Authentication security service. The security service may be required on any of links 1-2, 2-3, 3-4, or 4-5 in Figure 6/X.402.

10.2.4.2 *Content Integrity security service*

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

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

The Content Integrity security element together with the Message Argument Integrity security element and, in some cases, the Message Argument Confidentiality security element can be used to provide the security service to a message recipient, i.e., for communication from MTS-user 1 to MTS-user 5 in Figure 6/X.402. The Content Integrity security element is used to compute a Content Integrity Check as a function of the entire message content. Depending on the method used to compute the Content Integrity Check, a secret key may be required, which may be confidentially sent to the message recipient using the Message Argument Confidentiality security element. The Content Integrity Check is protected against change using the Message Argument Integrity security element. The integrity of any confidential message arguments is provided using the Message Argument Confidentiality security element.

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

10.2.4.3 *Message Sequence Integrity security service*

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

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

These security elements provide the service for communication from MTS-user 1 to MTS-user 5 in Figure 6/X.402, and not to the intermediate MTAs.

10.2.5 *Non-repudiation security services*

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

10.2.5.1 *Non-repudiation of origin security service*

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

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

The Content Integrity security element together with the Message Argument Integrity security element and, in some cases, the Message Argument Confidentiality security element can be used to provide the service to a message recipient, i.e., for communication from MTS-user 1 to MTS-user 5 in Figure 6/X.402. The Content Integrity security element is used to compute a Content Integrity Check as a function of the entire message content. Depending on the method used to compute the Content Integrity Check, a secret key may be required, which may be confidentially sent to the message recipient using the Message Argument Confidentiality security element. The Content Integrity Check and, if required, the Message Security Label are protected against change and/or repudiation using the Message Argument Integrity security element. Any confidential message arguments are protected against change and/or repudiation using the Message Argument Confidentiality security element.

If the Content Confidentiality security service is not required, the Message Origin Authentication security element may also be used as a basis for this security service. In this case the security service may be provided to all elements of the MHS, i.e., for all of 1-5 in Figure 6/X.402.

10.2.5.2 *Non-repudiation of Submission security service*

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

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

10.2.5.3 *Non-repudiation of Delivery security service*

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

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

10.2.6 *Message Security Labelling security service*

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

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

10.2.7 *Security management services*

A number of security management services are needed by the MHS. The only management services provided within Recommendation X.411 are concerned with changing credentials and registering MTS-user security labels.

10.2.7.1 *Change Credentials security service*

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

10.2.7.2 *Register security service*

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

10.2.7.3 *MS-register security service*

The security service enables the establishment of the security label which ar permissible for the MS-user.

10.3 *Security elements*

The following clauses describe the security elements available in the protocols described within Recommendation X.411 to support the security services in the MHS. These security elements relate directly to arguments in various services described in Recommendation X.411. The objective of this clause is to separate out each element of the Recommendation X.411 service definitions that relate to security, and to define the function of each of these identified security elements.

10.3.1 *Authentication security elements*

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

10.3.1.1 *Authentication exchange security element*

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

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

10.3.1.2 *Data Origin Authentication security elements*

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

10.3.1.2.1 *Message Origin Authentication security element*

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

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

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

10.3.1.2.2 *Probe Origin Authentication security element*

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

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

10.3.1.2.3 *Report Origin Authentication security element*

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

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

10.3.1.3 *Proof of Submission security element*

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

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

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

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

10.3.1.4 *Proof of Delivery security element*

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

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

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

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

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

10.3.2 *Secure Access Management security elements*

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

10.3.2.1 *Security Context security element*

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

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

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

10.3.2.2 *Register security element*

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

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

10.3.2.3 *MS-Register security element*

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

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

10.3.3 *Data Confidentiality security elements*

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

10.3.3.1 *Content Confidentiality security element*

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

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

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

10.3.3.2 *Message Argument Confidentiality security element*

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

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

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

10.3.4 *Data Integrity security elements*

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

10.3.4.1 *Content Integrity security element*

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

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

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

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

10.3.4.2 *Message Argument Integrity security element*

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

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

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

10.3.4.3 *Message Sequence Integrity security element*

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

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

10.3.5 *Non-repudiation security elements*

There are no specific Non-repudiation security elements defined in Recommendation X.411. The non-repudiation services may be provided using a combination of other security elements.

10.3.6 *Security Label security elements*

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

10.3.6.1 *Message Security Label security element*

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

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

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

10.3.7 *Security Management security elements*

10.3.7.1 *Change Credentials security element*

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

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

10.3.8 *Double Enveloping Technique*

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

This technique is available though the use of the Content Type argument which makes it possible to specify that the content of a message is an Inner Envelope. This Content Type means that the content is itself a message (envelope and content) for forwarding by the recipient named on the outer envelope to the recipient named on the Inner Envelope.

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

SECTION 3 – CONFIGURATIONS

11 Overview

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

This section covers the following topics:

a) functional configurations;

b) physical configurations;

c) organizational configurations;

d) the *Global MHS*.

12 Functional configurations

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

12.1 *Regarding the Directory*

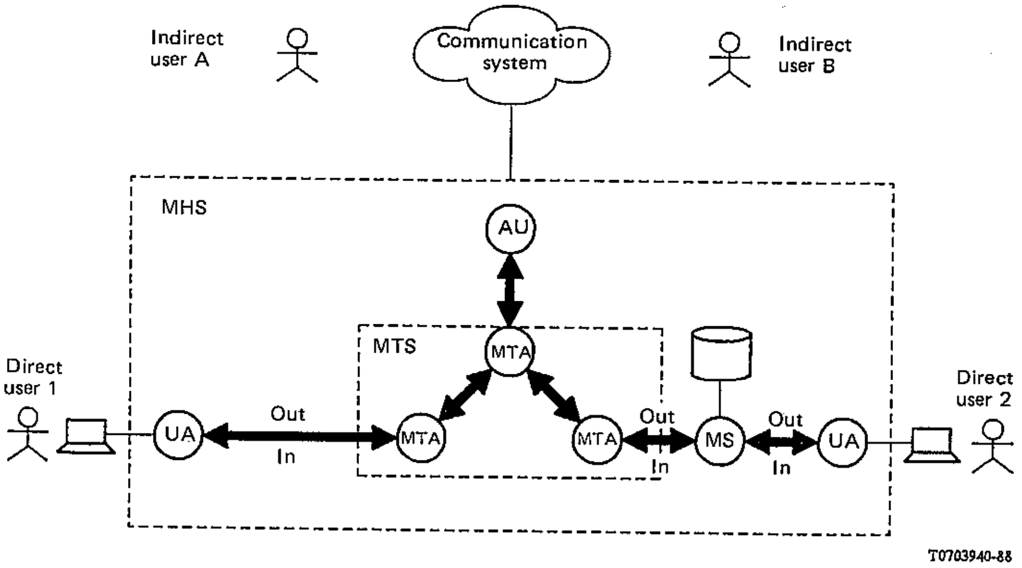
With respect to the Directory, the MHS can be configured for a particular user, or a collection of users (e.g., see § 14.1), in either of two ways: with or without the Directory. A user without access to the Directory may lack the capabilities described in Section 5.

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

12.2 *Regarding the message store*

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

The two functional configurations identified above are depicted in Figure 7/X.402 which also illustrates one possible configuration of the MTS, and its linkage to another communication system via an AU. In the figure, user 2 is equipped with an MS while user 1 is not.



Note – Whilde the users depicted in the Figure are people, the Figure applies with equal force and validity to users of other kinds.

FIGURE 7/X.402

Functional configurations regarding the MS

13 Physical configurations

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

13.1 *Messaging systems*

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

Messaging systems are of the types depicted in Figure 8/X.402.

The types of messaging system, depicted in Figure 8/X.402, are listed in the first column of Table 8/X.402. For each type listed, the second column indicates the kinds of functional object - UAs, MSs, MTAs, and AUs - that may be present in such a messaging system, whether their presence is mandatory or optional, and whether just one or possibly several of them may be present in the messaging system. The table is divided into two sections. Messaging systems of the types in the first section are dedicated to single users, those of the types in the second can (but need not) serve multiple users.

Table 8/X.402 is divided into two sections. Messaging systems of the types in the first section are dedicated to single users, those of the types in the second can (but need not) serve multiple users.

Note - The following major principles governed the admission of messaging system types:

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

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

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

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

The messaging system types, summarized in Table 8/X.402, are individually defined and described below.

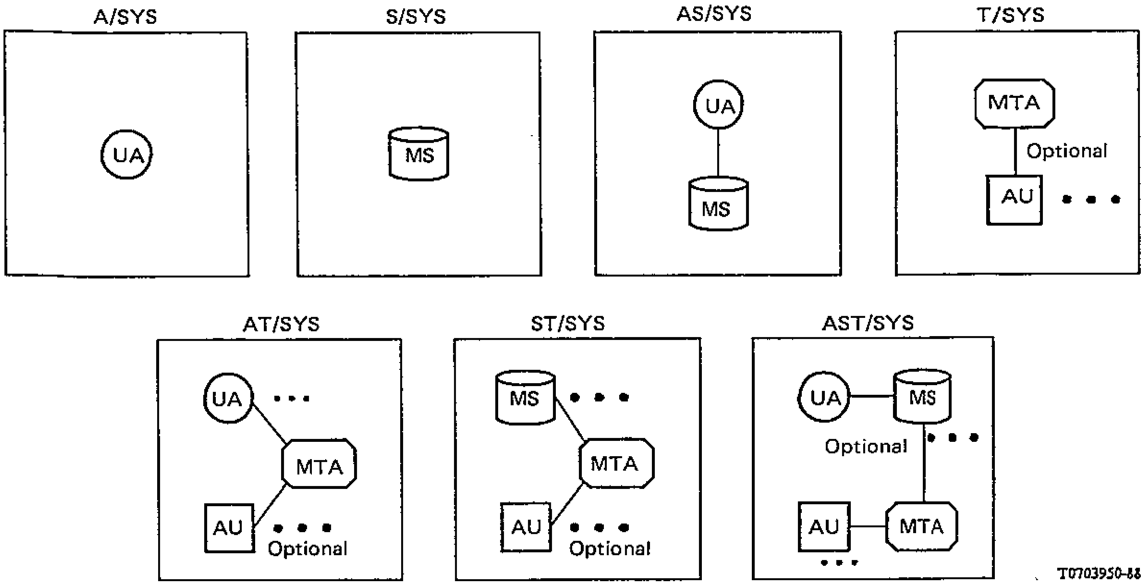


FIGURE 8/X.402

Messaging system types

TABLE 8/X.402

Messaging systems

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

M	Multiple
[. . .]	Optional

13.1.1 *Access systems*

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

An A/SYS is dedicated to a single user.

13.1.2 *Storage systems*

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

An S/SYS is dedicated to a single user.

13.1.3 *Access and storage systems*

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

An AS/SYS is dedicated to a single user.

13.1.4 *Transfer systems*

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

A T/SYS can serve multiple users.

13.1.5 *Access and transfer systems*

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

An AT/SYS can serve multiple users.

13.1.6 *Storage and transfer systems*

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

An ST/SYS can serve multiple users.

13.1.7 *Access, storage, and transfer systems*

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

An AST/SYS can serve multiple users.

13.2 *Representative configurations*

Messaging systems can be combined in various ways to form the MHS. The possible physical configurations are unbounded in number and thus cannot be enumerated. Several important representative configurations, however, are described below and in Figure 9/X.402.

13.2.1 *Fully centralized*

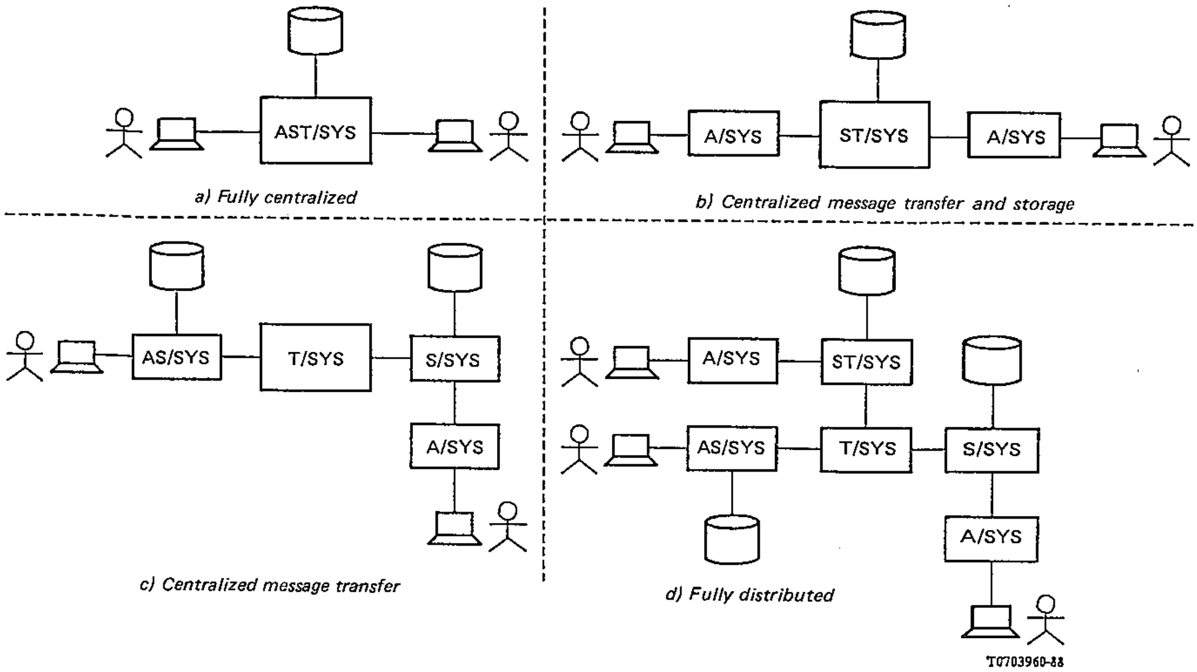
The MHS may be fully centralized [panel a) of Figure 9/X.402]. This design is realized by a single AST/SYS which contains functional objects of all kinds and which can serve multiple users.

13.2.2 *Centralized message transfer and storage*

The MHS may provide both message transfer and message storage centrally but user access distributedly [panel b) of Figure 9/X.402]. This design is realized by a single ST/SYS and, for each user, an A/SYS.

13.2.3 *Centralized message transfer*

The MHS may provide message transfer centrally but message storage and user access distributedly [panel c) of Figure 9/X.402]. This design is realized by a single T/SYS and, for each user, either an AS/SYS alone or an S/SYS and an associated A/SYS.



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

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

FIGURE 9/X.402

Representative physical configurations

13.2.4 *Fully distributed*

The MHS may provide even message transfer distributedly [panel d) of Figure 9/X.402]. This design involves multiple ST-SYSs or T-SYSs.

14 Organizational configurations

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

14.1 *Management domains*

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

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

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

14.1.1 *Administration management domains*

An **administration management domain (ADMD)** comprises messaging systems managed by an Administration. The major technical distinction between an ADMD and a *PRMD* is that the former is positioned above the latter in the MHS' hierarchical addressing (see § 18) and routing (see § 19) regimes.

Note – An ADMD provides Message Handling to the public.

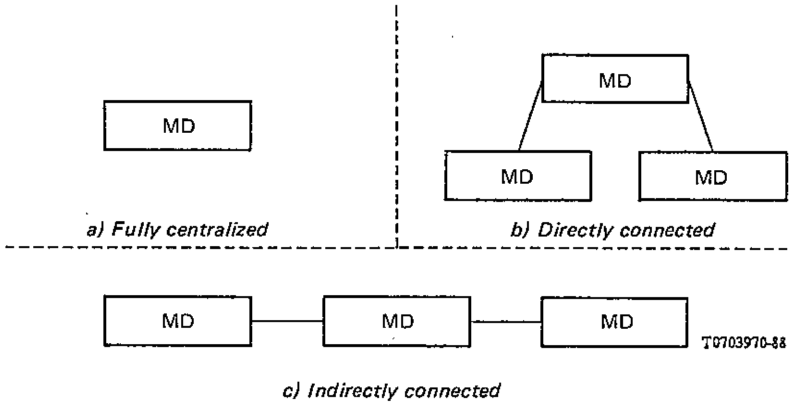
14.1.2 *Private management domains*

A **private management domain (PRMD)** comprises messaging systems managed by an organization other than an Administration. The major technical distinction between a PRMD and an ADMD is that the former is positioned below the latter in the MHS' hierarchical addressing (see § 18) and routing (see § 19) regimes.

Note – A PRMD provides message handling, e.g., to the employees of a company, or to those employees at a particular company site.

14.2 *Representative configurations*

MDs can be combined in various ways to form the MHS. The possible organizational configurations are unbounded in number and thus cannot be enumerated. Several important representative configurations, however, are described below and in Figure 10/X.402.



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

FIGURE 10/X.402

Representative organizational configurations

14.2.1 *Fully centralized*

The entire MHS may be managed by one organization [panel a) of Figure 10/X.402]. This design is realized by a single MD.

14.2.2 *Directly connected*

The MHS may be managed by several organizations, the messaging systems of each connected to the messaging systems of all of the others [panel b) of Figure 10/X.402]. This design is realized by multiple MDs interconnected pair-wise.

14.2.3 *Indirectly connected*

The MHS may be managed by several organizations, the messaging systems of one serving as intermediary between the messaging systems of the others [panel c) of Figure 10/X.402]. This design is realized by multiple MDs one of which is interconnected to all of the others.

15 The Global MHS

A major purpose of this Recommendation and others in the set is to enable the construction of the Global MHS, an MHS providing both intra- and inter-organizational, and both intra- and international message handling world-wide.

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

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

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

Figure 11/X.402 gives an example of possible interconnections. It does not attempt to identify all possible configurations. As depicted, ADMDs play a central role in the Global MHS. By interconnecting to one another internationally, they provide an international message transfer backbone. Depending upon national regulations, by interconnecting to one another domestically, they may also provide domestic backbones joined to the international backbone. ADMDs also serve as primary naming authorities in the assignment of *O/R addresses* to users and DLs.

PRMDs play a peripheral role in the Global MHS, being connected to the ADMD backbone which serves as an intermediary between them.

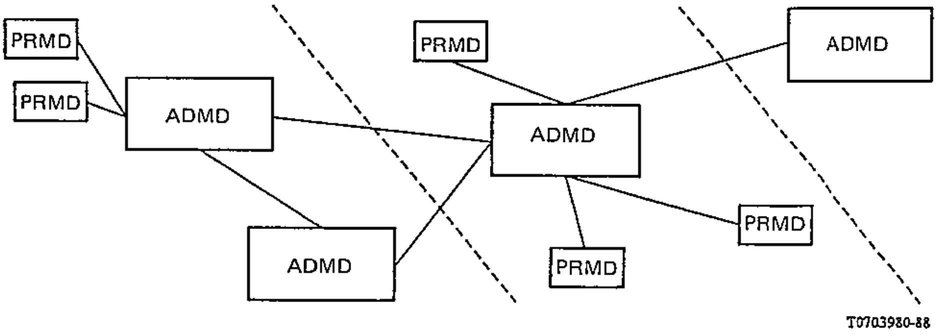


FIGURE 11/X.402

The global MHS

SECTION 4 – NAMING, ADDRESSING, AND ROUTING

16 Overview

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

This section covers the following topics:

a) Naming;

b) Addressing;

c) Routing

17 Naming

This paragraph specifies how users and DLs are named for the purposes of message handling in general and message transfer in particular. It defines *O/R names* and describes the role that Directory names play in them.

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

17.1 *Directory names*

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

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

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

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

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

17.2 *O/R names*

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

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

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

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

Note – Redirection or DL expansion may cause the MTS to convey to a UA or MS at delivery, O/R names the UA or MS did not supply at direct submission.

18 Addressing

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

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

18.1 *Attribute lists*

The *O/R addresses* of both users and DLs are attribute lists. An **attribute list** is an ordered set of *attributes*.

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

An attribute has the following parts:

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

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

Attributes are of the following two kinds:

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

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

b) **domain-defined attribute**: An attribute whose type is bound to a class of information by an MD.

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

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

18.2 *Character sets*

Standard attribute values and domain-defined attribute types and values are constructed from numeric, printable, and teletex strings as follows:

a) The type or value of a particular domaindefined attribute may be a printable string, a teletex string, or both. The same choice shall be made for both the type and value.

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

The value of an attribute comprises strings of one of the following sets of varieties depending upon its type: numeric only, printable only, numeric and printable, and printable and teletex. With respect to this, the following rules govern each instance of communication:

a) Wherever both numeric and printable strings are permitted, strings of either variety (but not both) may be supplied equivalently.

b) Wherever both printable and teletex strings are permitted, strings of either or both varieties may be supplied, but printable strings shall be supplied as a minimum whenever attributes are conveyed internationally. If both printable and teletex strings are supplied, the two should convey the same information so that eiher of them can be safely ignored upon receipt.

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

Note 1 – Teletex strings are permitted in attribute values to allow inclusion, e.g., of the accented characters commonly used in many countries.

Note 2 – Not all input/output devices permit the entry and display, e.g., of accented characters. printable strings are required internationally to ensure that such device limitations do not prevent communication.

18.3 *Standard attributes*

The standard attribute types are listed in the first column of Table 9/X.402. For each listed type, the second column indicates the character sets - numeric, printable, and teletex - from which attribute values may be drawn.

Table 9/X.402 has three sections. Attribute types in the first are of a general nature, those in the second have to do with *routing to* a PDS, and those in the third have to do with *addressing within* a PDS.

TABLE 9/X.402

Standard attributes

Standard attribute type	Character sets		
	NUM	PRT	TTX
General			
administration-domain-name	×	×	–
common-name	–	×	×
country-name	×	×	–
network-address	× [a]	–	–
numeric-user-identifier	×	–	–
organization-name	–	×	×
organizational-unit-names	–	×	×
personal-name	–	×	×
private-domain-name	×	×	–
terminal-identifier	–	×	–
terminal-type	–	–	–
Postal routing			
physical-delivery-service-name	–	×	–
physical-delivery-country-name	×	×	–
postal-code	×	×	–
Postal addressing			
extension-postal-O/R-address-components	–	×	×
extension-physical-delivery-address-components	–	×	×
local-postal-attributes	–	×	×
physical-delivery-office-name	–	×	×
physical-delivery-office-number	–	×	×
physical-delivery-organization-name	–	×	×
physical-delivery-personal-name	–	×	×
post-office-box-address	–	×	×
poste-restante-address	–	×	×
street-address	–	×	×
unformatted-postal-address	–	×	×
unique-postal-name	–	×	×

NUM	Numeric
PRT	Printable
TTX	Teletex
×	Permitted
[a]	Under prescribed circumstances a sequence of octet strings

The standard attribute types, summarized in Table 9/X.402, are individually defined and described below.

18.3.1 *Administration-domain-name*

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

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

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

18.3.2 *Common-name*

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

The value of a common-name is a printable string, teletex string, or both. Whether printable or teletex, the string is chosen from a set of such strings that is administered for this purpose (and perhaps others) by the entity alluded to above.

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

18.3.3 *Country-name*

A **country-name** is a standard attribute that identifies a country.

The value of a country-name is a numeric string that gives one of the numbers assigned to the country by Recommendation X.121, or a printable string that gives the character pair assigned to the country by ISO 3166.

18.3.4 *Extension-postal-O/R-address-components*

An **extension-postal-O/R-address-components** is a standard attribute that provides, in a postal address, additional information necessary to identify the addressee (e.g., an organizational unit).

The value of an extension-O/R-address-components is a printable string, teletex string, or both.

18.3.5 *Extension-physical-delivery-address-components*

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

The value of an extension-physical-delivery-address-components is a printable string, teletex string, or both.

18.3.6 *Local-postal-attributes*

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

The value of a local-postal-attributes is a printable string, teletex string, or both.

18.3.7 *Network-address*

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

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

a) a numeric string governed by Recommendation X.121;

b) two numeric strings governed by Recommendations E.163 and E.164;

c) a PSAP address.

Note – Among the strings admitted by Recommendation X.121 is a telex number preceded by the telex escape digit (8).

18.3.8 *Numeric-user-identifier*

A **numeric-user-identifier** is a standard attribute that numerically identifies a user relative to the ADMD denoted by an administration-domain-name.

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

18.3.9 *Organization-name*

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

The value of an organization-name is a printable string, teletex string, or both. Whether printable or teletex, the string is chosen from a set of such strings that is administered for this purpose (and perhaps others) by the country or MD alluded to above.

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

18.3.10 *Organizational-unit-names*

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

The value of an organizational-unit-names is an ordered sequence of printable strings, an ordered sequence of teletex strings, or both. Whether printable or teletex, each string is chosen from a set of such strings that is administered for this purpose (and perhaps others) by the organization (or encompassing unit) alluded to above.

18.3.11 *Physicel-delivery-service-name*

A **physical-delivery-service-name** is a standard attribute that identifies a PDS relative to the ADMD denoted by an administration-domain-name.

The value of a physical-delivery-service-name is a printable string chosen from a set of such strings that is administered for this purpose by the ADMD alluded to above.

18.3.12 *Personal-name*

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

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

a) the person's surname;

b) the person's given name;

c) the initials of all of his names but his surname;

d) his generation (e.g., “Jr”).

The above information is supplied as printable strings, teletex strings, or both.

18.3.13 *Physical-delivery-country-name*

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

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

18.3.14 *Physical-delivery-office-name*

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

The value of a physical-delivery-office-name is a printable string, teletex string, or both.

18.3.15 *Physical-delivery-office-number*

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

The value of a physical-delivery-office-number is a printable string, teletex string, or both.

18.3.16 *Physical-delivery-organization-name*

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

The value of a physical-delivery-organization-name is a printable string, teletex string, or both.

18.3.17 *Physical-delivery-personal-name*

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

The value of a physical-delivery-personal-name is a printable string, teletex string, or both.

18.3.18 *Post-office-box-address*

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

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

18.3.19 *Postal-code*

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

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

18.3.20 *Poste-restante-address*

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

The value of a poste-restante-address is a printable string, teletex string, or both chosen from the set of such strings assigned for this purpose by the post office denoted by a physical-delivery-office-name attribute.

18.3.21 *Private-domain-name*

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

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

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

18.3.22 *Street-address*

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

The value of a street-address is a printable string, teletex string, or both.

18.3.23 *Terminal-identifier*

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

The value of a terminal-identifier is a printable string.

18.3.24 *Terminal-type*

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

The value of a terminal-type is any one of the following: *telex, teletex, G3 facsimile, G4 facsimile, IA5 terminal,* and *videotex*.

18.3.25 *Unformatted-postal-address*

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

The value of an unformatted-postal address is a sequence of printable strings, each representing a line of text, a single teletex string, lines being separated as prescribed for such strings; or both.

18.3.26 *Unique-postal-name*

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

The value of a unique-postal-name is a printable string, teletex string, or both.

18.4 *Attribute list equivalence*

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

a) The relative order of standard attributes is insignificant.

b) Where the value of a standard attribute may be a numeric string or an equivalent printable string, the choice between them shall be considered insignificant.

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

c) Where the value of a standard attribute may be a printable string, an equivalent teletex string, or both, the choice between the three possibilities shall be considered insignificant.

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

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

Note 1 – An MD may impose additional equivalence rules upon the attributes it assigns to its own users and DLs. It might define, e.g., rules concerning punctuation characters in attribute values, the case of letters in such values, or the relative order of domain-defined attributes.

Note 2 – As a national matter, MDs may impose additional equivalence rules regarding standard attributes whose values are given as teletex strings, in particular, the rules for deriving the equivalent printable strings.

18.5 *O/R address forms*

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

An O/R address may take any of the forms summarized in Table 10/X.402. The first column of the table identifies the attributes available for the construction of O/R addresses. For each O/R address form, the second column indicates the attributes that may appear in such O/R addresses and their grades (see also § 18.6).

Table 10/X.402 has four sections. Attribute types in the first are those of a general nature, attribute types in the second and third those specific to physical delivery. The fourth section encompasses domain-defined attributes.

The forms of O/R address, summarized in Table 10/X.402 are individually defined and described below.

18.5.1 *Mnemonic O/R address*

A **mnemonic O/R address** is one that mnemonically identifies a user or DL. It identifies an ADMD, and a user or DL relative to it.

A mnemonic O/R address comprises the following attributes:

a) one country-name and one administration-domain-name, which together identify an ADMD;

b) one private-domain-name, one organization-name, one organizational-unit-names, one personal-name or common-name, or a combination of the above; and optionally one or more domain-defined attributes; which together identify a user or DL relative to the ADMD in item a) above.

18.5.2 *Numeric O/R address*

A **numeric O/R address** is one that numerically identifies a user. It identifies an ADMD, and a user relative to it.

A numeric O/R address comprises the following attributes:

a) one country-name and one administration-domain-name, which together identify an ADMD;

b) one numeric-user-identifier and, conditionally, one private-domain-name, which together identify the user relative to the ADMD in item a above;

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

18.5.3 *Postal O/R address*

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

The following kinds of postal O/R address are distinguished:

a) **formatted**;: Said of a postal O/R address that specifies a user's postal address by means of several attributes. For this form of postal O/R address, this Recommendation prescribes the structure of postal addresses in some detail;

b) **unformatted**;: Said of a postal O/R address that specifies a user's postal address in a single attribute. For this form of postal O/R address, this Recommendation largely does not prescribe the structure of postal addresses.

TABLE 10/X.402

Forms of O/R address

Attribute type	O/R address forms				
	MNEM	NUMR	POST		TERM
			F	U	
General					
administration-domain-name	M	M	M	M	C
Common-name	C	—	—	—	—
country-name	M	M	M	M	C
network-address	—	—	—	—	M
numeric-user-identifier	—	M	—	—	—
organization-name	C	—	—	—	—
organizational-unit-names	C	—	—	—	—
Personal-name	C	—	—	—	—
private-domain-name	C	C	C	C	C
Terminal-identifier	—	—	—	—	C
Terminal-identifier	—	—	—	—	C
Postal routing					
Physical-delivery-service	—	—	C	C	—
Physical-delivery-country-name	—	—	M	M	—
postal-code	—	—	M	M	—
Postal addressing					
extension-postal-O/R-address-components	—	—	C	—	—
extension-physical-delivery-address-components	—	—	C	—	—
local-postal-attributes	—	—	C	—	—
Physical-delivery-office-name	—	—	C	—	—
Physical-delivery-office-number	—	—	C	—	—
Physical-delivery-organization-name	—	—	C	—	—
Physical-delivery-personal-name	—	—	C	—	—
poste-office-box-address	—	—	C	—	—
poste-restante-address	—	—	C	—	—
street address	—	—	C	—	—
unformatted-postal-address	—	—	—	M	—
unique-postal-name	—	—	C	—	—
Domain-defined					
domain-defined (one or more)	C	C	—	—	C

MNEM	Mnemonic	F	Formatted
NUMR	Numeric	U	Unformatted
POST	Postal	M	Mandatory
TERM	Terminal	C	Conditional

A postal O/R address, whether formatted or unformatted, comprises the following attributes:

a) one country-name and one administration-domain-name, which together identify an ADMD;

b) conditionally, one private-domain-name, one physical-delivery-service-name, or both, which together identify the PDS by means of which the user is to be accessed;

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

A formatted postal O/R address comprises, additionally, one of each postal addressing attribute (see Table 9/X.402), except unformatted-postal-address, that the PDS requires to identify the postal patron.

An unformatted postal O/R address comprises, additionally, one unformatted-postal-address attribute.

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

18.5.4 *Terminal O/R address*

A **terminal O/R address** is one that identifies a user by means of the network address and, if required, the type of his terminal. It may also identify the ADMD through which that terminal is accessed. In the case of a telematic terminal, it gives the terminal's network address and possibly its terminal identifier and terminal type. In the case of a telematic terminal, it gives the terminal's network address and possibly its terminal identifier and terminal type. In the case of a telex terminal, it gives its telex number.

A terminal O/R address comprises the following attributes:

a) one network-address;

b) conditionally, one terminal-identifier;

c) conditionally, one terminal-type;

d) conditionally, both one country-name and one administration-domain-name which together identify an ADMD;

e) conditionally, one private-domain-name and, conditionally, one or more domain-defined attributes, all of which provide information additional to that which identifies the user.

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

18.6 *Conditional attributes*

The presence or absence in a particular O/R address of the attributes marked conditional in Table 10/X.402 is determined as follows.

If a user or DL is accessed through a PRMD, attributes used to route messages to the PRMD are present in the O/R address at the discretion of, and in accordance with rules established by the ADMD denoted by the country-name and administration-domain-name attributes of the O/R address. The ADMD imposes no other constraints on the attributes in the O/R address. If a user is not accessed through a PRMD, all conditional attributes except those specific to postal O/R addresses are present in an O/R address at the discretion of, and in accordance with rules established by, the ADMD denoted by the country-name and administration-domain-name attributes.

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

19 Routing

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

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

The following principles are illustrative, not definitive:

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

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

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

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

e) When the MD is directly connected to the MD identified by the O/R address, the object is typically routed to that MD directly.

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

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

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

SECTION 5 – USE OF THE DIRECTORY

20 Overview

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

This section covers the following topics:

a) authentication;

b) name resolution;

c) DL expansion;

d) capability assessment.

21 Authentication

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

22 Name resolution

A functional object may accomplish name resolution using the Directory.

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

a) *MHS O/R addresses;*

b) *MHS preferred delivery methods*

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

23 DL expansion

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

To obtain the members of a DL whose Directory name it possesses, the object presents that name to the Directory and requests from the object's Directory entry the following attributes:

a) *MHS DL members;*

b) *MHS DL submit permissions;*

c) *MHS preferred delivery methods.*

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

24 Capability assessment

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

The following Directory attributes represent user capabilities of possible significance in message handling:

a) *MHS deliverable content length;*

b) *MHS deliverable content types;*

c) *MHS deliverable EITs;*

d) *MHS preferred delivery methods.*

The following Directory attributes represent MS capabilities of possible significance in message handling:

a) *MHS supported automatic actions*;

b) *MHS supported content types*;

c) *MHS supported optional attributes*.

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

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

SECTION 6 – OSI REALIZATION

25 Overview

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

This section covers the following topics:

a) application service elements;

b) application contexts.

26 Application service elements

This paragraph identifies the application service elements(ASEs) that figure in the OSI realization of message handling.

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

Note – Besides the ASEs discussed, the MHS relies upon the Directory access service element defined in Recommendation X.519. However, since that ASE does not figure in the ACs for message handling (see Recommendation X.419), it is not discussed here.

26.1 *The ASE concept*

The ASE concept is illustrated in Figure 12/X.402, which depicts two communicating open systems. Only the OSI-related portions of the open systems, called AEs, are shown. Each AE comprises a UE and one or more ASEs. A UE represents the controlling or organizing portion of an AE which defines the open system's role (e.g., that of an MTA). An ASE represents one of the communication capability sets, or services (e.g., for message submission or transfer), that the UE requires to play its role.

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

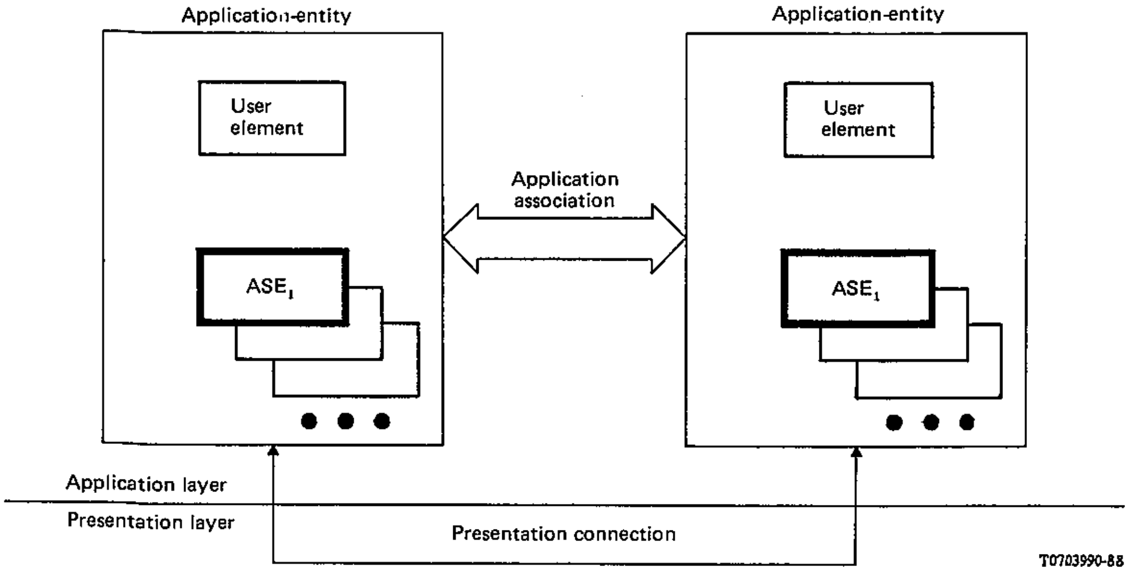


FIGURE 12/X.402

The ASE concept

An ASE plays the largely mechanical role of translating requests and responses made by its UE to and from the form dictated by the application protocol that governs the ASE's interaction with its peer ASE in the open system to which the association connects it. The ASE realizes an abstract service, or a part thereof, for purposes of OSI communication (see Recommendation X.407).

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

26.2 *Symmetric and asymmetric ASEs*

The following two kinds of ASE, illustrated in Figure 13/X.402, can be distinguished:

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

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

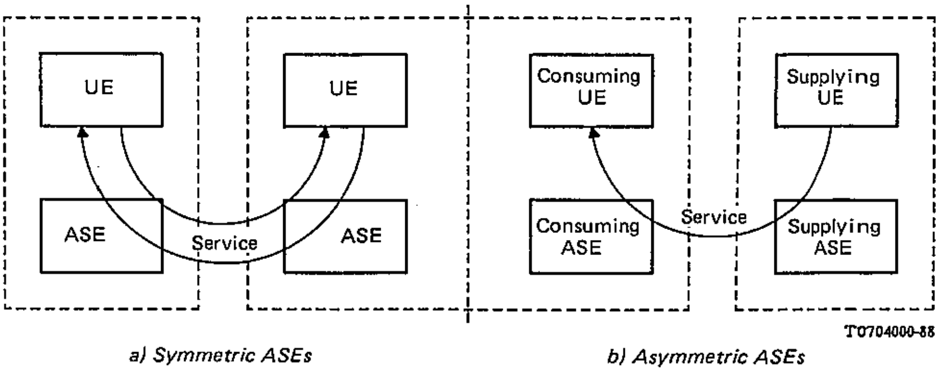


FIGURE 13/X.402

Symmetric and asymmetric ASEs

With respect to a particular asymmetric ASE, one UE supplies a service which the other consumes. The ASEs co-located with the UEs assist in the service's supply and consumption. The resulting four roles are captured in Figure 14/X.402 and in the following terminology:

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

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

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

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

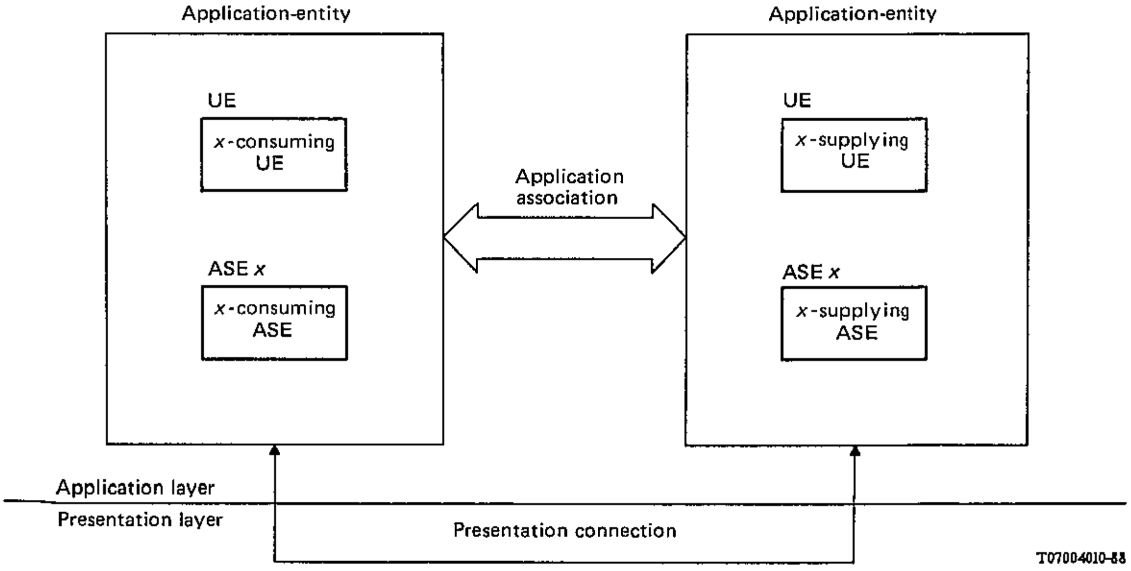


FIGURE 14/X.402

Terminology for asymmetric ASEs

As indicated, the four roles described above are defined relative to a particular ASE. When an AE comprises several asymmetric ASEs, these roles are assigned independently for each ASE. Thus, as shown in Figure 15/X.402, a single UE might serve as the consumer with respect to one ASE and as the supplier with respect to another.

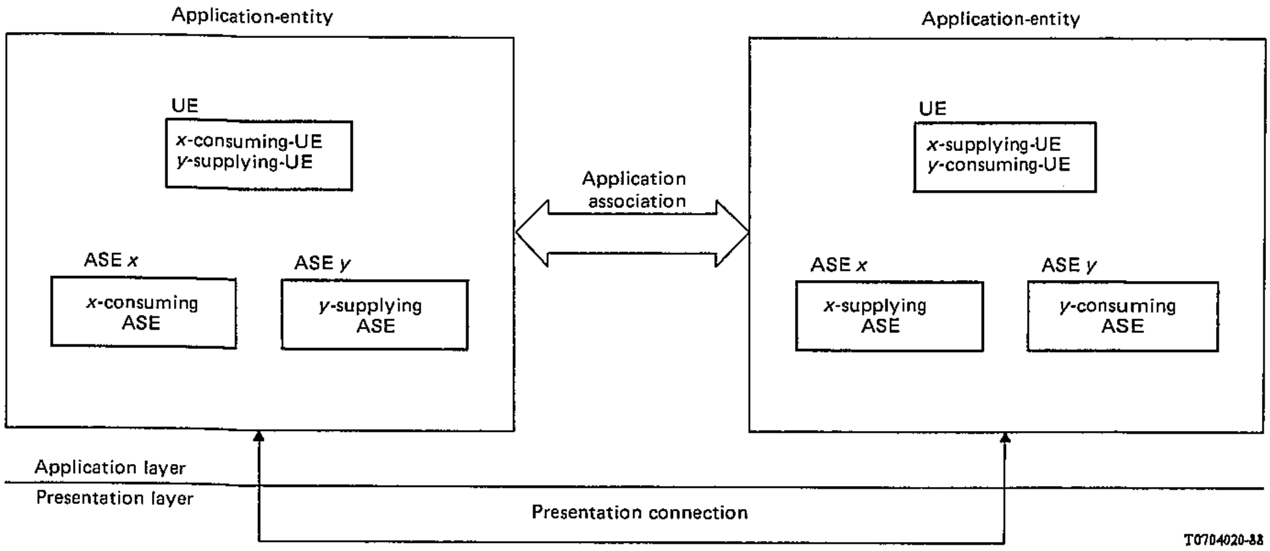


FIGURE 15/X.402

Multiple asymmetric ASEs

26.3 *Message handling ASEs*

The ASEs that provide the various message handling services are listed in the first column of Table 11/X.402. For each ASE listed, the second column indicates whether it is symmetric or asymmetric. The third column identifies the functional objects - UAs, MSs, MTAs, and AUs - that are associated with the ASE, either as consumer or as supplier.

TABLE 11/X.402

Message handling ASEs

ASE	Form	Functional objects			
		UA	MS	MTA	AU
MTSE	SY	—	—	CS	—
MSSE	ASY	C	CS	S	—
MDSE	ASY	C	CS	S	—
MRSE	ASY	C	SS	-	—
MASE	ASY	C	CS	S	—

SY	Symmetric
ASY	Asymmetric
C	Consumer
S	Supplier

The message handling ASEs, summarized in Table 11/X.402, are individually introduced in the clauses below. Each is defined in Recommendation X.419.

26.3.1 *Message transfer*

The message transfer service element (MTSE) is the means by which the transfer transmittal step is effected.

26.3.2 *Message submission*

The message submission service element (MSSE) is the means by which the submission transmittal step is effected.

26.3.3 *Message delivery*

The message delivery service element (MDSE) is the means by which the delivery transmittal step is effected.

26.3.4 *Message retrieval*

The message retrieval service element (MRSE) is the means by which the retrieval transmittal step is effected.

26.3.5 *Message administration*

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

26.4 *Supporting ASEs*

The general-purpose ASEs upon which message handling ASEs depend are listed in the first column of Table 12/X.402. For each listed ASE, the second column indicates whether it is symmetric or asymmetric.

TABLE 12/X.402

Supporting ASEs

ASE	Form
ROSE	SY
RTSE	SY
ACSE	SY

SY Symmetric

The supporting ASEs, summarized in Table 12/X.402 are individually introduced below.

26.4.1 *Remote operations*

The remote operations service element (ROSE) is the means by which the asymmetric Message Handling ASEs structure their request-response interactions between consuming and supplying open systems.

The ROSE is defined in Recommendation X.219.

26.4.2 *Reliable transfer*

The reliable transfer service element (RTSE) is the means by which various symmetric and asymmetric message handling ASEs convey information objects - especially large ones (e.g., facsimile messages) - between open systems so as to ensure their safe-storage at their destinations.

The RTSE is defined in Recommendation X.218.

26.4.3 *Association control*

The association control service element (ACSE) is the means by which all application associations between open systems are established, released, and in other respects managed.

The ACSE is defined in Recommendation X.217.

27 Application contexts

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

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

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

An AC also identifies by name (an ASN.1 object identifier) the abstract syntaxes of the APDUs that an association may carry as a result of its use by the AC's ASEs. Conventionally one assigns a name to the set of APDUs associated either with each individual ASE or with the AC as a whole. The initiator of an association indicates to the responder the one or more abstract syntaxes associated with the AC by conveying their names to it via the ACSE.

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

The ACs by means of which the various message handling services are provided are specified in Recommendation X.419. These protocols are known as P1, P3, and P7.

Note – The nature of a message's content does not enter into the definition of message handling ACs because the content is encapsulated (as an octet string) in the protocols by means of which it is conveyed.

ANNEX A

(to Recommendation X.402)

Directory object classes and attributes

This Annex is an integral part of this Recommendation.

Several Directory object classes, attributes, and attribute syntaxes are specific to Message Handling. These are defined in the present Annex using the OBJECT-CLASS, ATTRIBUTE, and ATTRIBUTE-SYNTAX macros of Recommendation X.501, respectively.

A.1 *Object classes*

The object classes specific to message handling are those specified below.

Note – The Directory object classes described in this Annex can be combined with other object classes, eg., the ones defined in Recommendation X.521. See also Recommendation X.501, § 9, for an explanation of how Directory object classes can be combined in one Directory entry. Annex B of Recommendation X.521 gives some further information about Directory name forms and possible Directory information tree structures.

A.1.1 *MHS distribution list*

An **MHS distribution list** object is a DL. The attributes in its entry identify its common name, submit permissions, and O/R addresses and, to the extent that the relevant attributes are present, describe the DL, identify its organization, organizational units, and owner; cite related objects; and identify its deliverable content types, deliverable EITs, members, and preferred delivery methods.

```
mhs-distribution-list OBJECT-CLASS
    SUBCLASS OF top
    MUST CONTAIN {
        commonName,
        mhs-dl-submit-permissions,
        mhs-or-addresses}
    MAY CONTAIN {
        description,
        organization,
        organizationalUnitName,
        owner,
        seeAlso,
        mhs-deliverable-content-types,
        mhs-deliverable-eits,
        mhs-dl-members,
        mhs-preferred-delivery-methods }
    ::= id-oc-mhs-distribution-list
```

A.1.2 *MHS message store*

An **MHS message store** object is an AE that realizes an MS. The attributes in its entry, to the extent that they are present, describe the MS, identify its owner, and enumerate the optional attributes, automatic actions, and content types it supports.

```
mhs-message-store OBJECT-CLASS
    SUBCLASS OF applicationEntity
    MAY CONTAIN {
        description,
        owner,
        mhs-supported-optional-attributes,
        mhs-supported-automatic-actions,
        mhs-supported-content-types }
    ::= id-oc-mhs-message-store
```

A.1.3 *MHS message transfer agent*

An **MHS message transfer agent** object is an AE that implements an MTA. The attributes in its entry, to the extent that they are present, describe the MTA and identify its owner and its deliverable content length.

```
mhs-message-transfer-agent OBJECT-CLASS
    SUBCLASS OF applicationEntity
    MAY CONTAIN {
        description,
        owner,
        mhs-deliverable-content-length }
    ::= id-oc-mhs-message-transfer-agent
```

A.1.4 *MHS user*

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

```
mhs-user OBJECT-CLASS
    SUBCLASS OF top
    MUST CONTAIN {
        mhs-or-addresses }
    MAY CONTAIN {
        mhs-deliverable-content-length,
        mhs-deliverable-content-types,
        mhs-deliverable-eits,
        mhs-message-store,
        mhs-preferred-delivery-methods }
    ::= id-oc-mhs-user
```

A.1.5 *MHS user agent*

An **MHS user agent** object is an AE that realizes a UA. The attributes in its entry, to the extent that they are present, identify the UA's owner; its deliverable content length, content types, and EITs; and its O/R address.

```
mhs-user-agent OBJECT-CLASS
    SUBCLASS OF applicationEntity
    MAY CONTAIN {
        owner,
        mhs-deliverable-content-length,
        mhs-deliverable-content-types,
        mhs-deliverable-eits,
        mhs-or-addresses }
    ::= id-oc-mhs-user-agent
```

A.2 *Attributes*

The attributes specific to message handling are those specified below.

A.2.1 *MHS deliverable content length*

The **MHS deliverable content length** attribute identifies the maximum content length of the messages whose delivery a user will accept.

A value of this attribute is an Integer.

```
mhs-deliverable-content-length ATTRIBUTE
    WITH ATTRIBUTE-SYNTAX integerSyntax
    SINGLE VALUE
    ::= id-at-mhs-eliverable-content-length
```

A.2.2 *MHS deliverable content types*

The **MHS deliverable content types** attribute identifies the content types of the messages whose delivery a user will accept.

A value of this attribute is an object identifier.

```
mhs-deliverable-content-types ATTRIBUTE
    WITH ATTRIBUTE-SYNTAX objectIdentifierSyntax
    MULTI VALUE
    = id-at-mhs-liverable-content-types
```

A.2.3 *MHS deliverable EITs*

The **MHS deliverable EITs** attribute identifies the EITs of the messages whose delivery a user will accept.

A value of this attribute is an object identifier.

```
mhs-deliverable-eits ATTRIBUTE
    WITH ATTRIBUTE-SYNTAX objectIdentifierSyntax
    MULTI VALUE
    ::= id-at-mhs-deliverable-eits
```

A.2.4 *MHS DL members*

The **MHS DL members** attribute identifies a DL's members.

A value of this attribute is an O/R name.

```
mhs-dl-members ATTRIBUTE
    WITH ATTRIBUTE-SYNTAX mhs-or-name-syntax
    MULTI VALUE
    ::= id-at-mhs-dl-members
```

A.2.5 *MHS DL submit permissions*

The **MHS DL submit permissions** attribute identifies the users and DLs that may submit messages to a DL.

A value of this attribute is a DL submit permission.

```
mhs-dl-submit-permissions ATTRIBUTE
    WITH ATTRIBUTE-SYNTAX mhs-dl-submit-permission-syntax
    MULTI VALUE
    ::= id-at-mhs-dl-submit-permissions
```

A.2.6 *MHS message store*

The **MHS message store** attribute identifies a user's MS by name.

The value of this attribute is a Directory distinguished name.

```
mhs-message-store ATTRIBUTE
    WITH ATTRIBUTE-SYNTAX distinguishedNameSyntax
    SINGLE VALUE
    ::= id-at-mhs-message-store
```

A.2.7 *MHS O/R addresses*

The **MHS O/R addresses** attribute specifies a user's or DL's O/R addresses.

A value of this attribute is an O/R address.

```
mhs-or-addresses ATTRIBUTE

    WITH ATTRIBUTE-SYNTAX mhs-or-address-syntax
    MULTI VALUE
    ::= id-at-mhs-or-addresses
```

A.2.8 *MHS preferred delivery methods*

The **MHS preferred delivery methods** attribute identifies, in order of decreasing preference, the methods of delivery a user prefers.

A value of this attribute is a preferred delivery method.

```
mhs-preferred-delivery-methods ATTRIBUTE

    WITH ATTRIBUTE-SYNTAX RequestedDeliveryMethod
    MATCHES FOR EQUALITY
    SINGLE VALUE
    ::= id-at-mhs-preferred-delivery-methods
```

A.2.9 *MHS supported automatic actions*

The **MHS supported automatic actions** attribute identifies the automatic actions that an MS fully supports.

A value of this attribute is an object identifier.

```
mhs-supported-automatic-actions ATTRIBUTE

    WITH ATTRIBUTE-SYNTAX objectIdentifierSyntax
    MULTI VALUE
```

```
          ::= id-at-mhs-supported-automatic-actions
```

A.2.10 *MHS supported content types*

The **MHS supported content types** attribute identifies the content types of the messages whose syntax and semantics a MS fully supports.

A value of this attribute is an object identifier.

```
mhs-supported-content-types ATTRIBUTE
     WITH ATTRIBUTE-SYNTAX objectIdentifierSyntax
     MULTI VALUE
     ::= id-at-mhs-supported-content-types
```

A.2.11 *MHS supported optional attributes*

The **MHS supported optional attributes** attribute identifies the optional attributes that an MS fully supports.

A value of this attribute is an Object Identifier.

```
mhs-supported-optional-attributes ATTRIBUTE

     WITH ATTRIBUTE-SYNTAX objectIdentifierSyntax
     MULTI VALUE
     ::= id-at-mhs-supported-optional-attributes
```

A.3 *Attribute syntaxes*

The attribute syntaxes specific to message handling are those specified below.

A.3.1 *MHS DL submit permission*

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

```
mhs-dl-submit-permission-syntax ATTRIBUTE-SYNTAX
     SYNTAX DLSubmitPermission
     MATCHES FOR EQUALITY
     ::= id-as-mhs-dl-submit-permission
```

```
DLSubmitPermission ::= CHOICE {
     individual           [0] ORName,
     member-of-dl         [1] ORName,

     pattern-match        [2] ORNamePattern,
     member-of-group      [3] Name }
```

A presented DL submit permission value shall be of type *Individual*.

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

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

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

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

```
ORNamePattern ::= ORName
```

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

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

A.3.2 *MHS O/R address*

The **MHS O/R address** attribute syntax characterizes an attribute each of whose values is an O/R address.

```
mhs-or-address-syntax ATTRIBUTE-SYNTAX
      SYNTAX ORAddress
      MATCHES FOR EQUALITY
      ::= id-as-mhs-or-address
```

A presented O/R address value is equal to a target O/R address value under the conditions specified in § 18.4.

A.3.3 *MHS O/R name*

The **MHS O/R name** attribute syntax characterizes an attribute each of whose values is an O/R name.

```
mhs-or-name-syntax ATTRIBUTE-SYNTAX
      SYNTAX ORName
      MATCHES FOR EQUALITY
      ::= id-as-mhs-or-name
```

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

ANNEX B

(to Recommendation X.402)

Reference definition of object identifiers

This Annex is an integral part of this Recommendation.

This Annex defines for reference purposes various object identifiers cited in the ASN.1 module of Annex C. It uses ASN.1.

All object identifiers this Recommendation assigns are assigned in this Annex. Annex B is definitive for all but those for ASN.1 modules and MHS itself. The definitive assignments for the former occur in the modules themselves; other references to them appear in IMPORT clauses. The latter is fixed.

```
MHSObjectIdentifiers { joint-iso-ccitt

            mhs-motis(6) arch(5) modules(0) object-identifiers(0) }
                  DEFINITIONS IMPLICIT TAGS ::=
                  BEGIN
                  -- Prologue
                  -- Exports everything.

IMPORTS -- nothing -- ;

ID ::= OBJECT IDENTIFIER

-- Aspects MHS

id-mhsac    ID ::= { joint-iso-ccitt mhs-motis(6) mhsac(0) }
            -- MHS Application Contexts
            -- See Recommendation X.419.

id-ipms     ID ::= { joint-iso-ccitt mhs-motis(6) ipms(1) }
            -- Interpersonal Messaging
            -- See Recommendation X.420.

id-asdc     ID ::= { joint-iso-ccitt mhs-motis(6) asdc(2) }
            -- Abstract Service Definition Conventions
            -- See Recommendation X.407.
```

```
id-mts     ID ::= { joint-iso-ccitt mhs-motis(6) mts(3) }
           -- Message Transfer System
           -- See Recommendation X.411.

id-ms      ID ::= { joint-iso-ccitt mhs-motis(6) ms(4) }
           -- Message Store
           -- See Recommendation X.413.

id-arch    ID ::= { joint-iso-ccitt mhs-motis(6) arch(5) }
           -- Overall Architecture
           -- See this Recommendation.

id-group   ID ::= { joint-iso-ccitt mhs0-motis(6) group(6) }
           -- Reserved.
-- Categories

id-mod     ID ::= { id-arch 0 } -- modules, not definitive

id-oc      ID ::= { id-arch 1 } -- object classes

id-at      ID ::= { id-arch 2 } -- attribute types

id-as      ID ::= { id-arch 3 } -- attribute syntaxes

-- Modules

id-object-identifiers                     ID ::= { id-mod 0 } -- not definitive

id-directory-objects-and-attributes;      ID ::= { id-mod 1 }

             -- not definitive

-- Object classes

id-oc-mhs-distribution-list               ID ::= { id-oc 0 }

id-oc-mhs-message-store                   ID ::= { id-oc 1 }

id-oc-mhs-message-transfer-agent          ID ::= { id-oc 2 }

id-oc-mhs-user                            ID ::= { id-oc 3 }

id-oc-mhs-user-agent                      ID ::= { id-oc 4 }

-- Attributes

id-at-mhs-deliverable-content-legth       ID ::= { id-at 0 }

id-at-mhs-deliverable-content-types       ID ::= { id-at 1 }

id-at-mhs-deliverable-eits                ID ::= { id-at 2 }

id-at-mhs-dl-members                      ID ::= { id-at 3 }

id-at-mhs-dl-submit-permissions           ID ::= { id-at 4 }

id-at-mhs-message-store                   ID ::= { id-at 5 }

id-at-mhs-or-addresses                    ID ::= { id-at 6 }

id-at-mhs-preferred-delivery-methods      ID ::= { id-at 7 }

id-at-mhs-supported-automatic-actions     ID ::= { id-at 8 }

id-at-mhs-supported-content-types         ID ::= { id-at 9 }

id-at-mhs-supported-optional-attributes   ID ::= { id-at 10 }
```

```
-- Attribute syntaxes
id-as-mhs-dl-submit-permission          ID ::= { id-as 0 }
id-as-mhs-or-address                    ID ::= { id-as 1 }
id-as-mhs-or-name                       ID ::= { id-as 2 }
END -- of MHSObjectIdentifiers
```

ANNEX C

(to Recommendation X.402)

Reference definition of directory object classes and attributes

This Annex is an integral part of this Recommendation.

This Annex, a supplement to Annex A, defines for reference purposes the object classes, attributes, and attribute syntaxes specific to Message Handling. It uses the OBJECT-CLASS, ATTRIBUTE, and ATTRIBUTE-SYNTAX macros of Recommendation X.501.

```
MHSDirectoryObjectsAndAttributes { joint-iso-ccitt
        mhs-motis(6) arch(5) modules(0) directory(1) }
DEFINITIONS IMPLICIT TAGS ::=
BEGIN
        -- Prologue
        -- Exports everything.
IMPORTS
        -- MHS object identifiers
                id-as-mhs-dl-submit-permission, id-as-mhs-or-address,
                id-as-mhs-or-name-, id-at-mhs-deliverable-content-length,
                id-at-mhs-deliverable-content-types,
                id-at-mhs-deliverable-eits, id-at-mhs-dl-members,
                id-at-mhs-dl-submit-permissions, id-at-mhs-message-store,
                id-at-mhs-or-addresses, id-at-mhs-preferred-delivery-methods,
                id-at-mhs-supported-automatic-actions,
                id-at-mhs-supported-content-types,
                id-at-mhs-supported-optional-attributes,
                id-oc-mhs-distribution-list, id-oc-mhs-message-store,
                id-oc-mhs-message-transfer-agent,
                id-oc-mhs-user,
                id-oc-mhs-user-agent
                ----
                FROM MHSObjectIdentifiers { joint-iso-ccitt
                    mhs-motis(6) arch(5) modules(0) object-identifiers(0) }
        -- MTS Abstract service
                ORAddress, ORName, RequestedDeliveryMethod
                ----

                FROM MTSAbstractService { joint-iso-ccitt
                    mhs-motis(6) mts(3) modules(0) MTS-abstract-service(3) }
```

```
    -- Information framework
        ATTRIBUTE, ATTRIBUTE-SYNTAX, Name, OBJECT-CLASS
        ----
        FROM informationFramework { joint-iso-ccitt
            ds(5) modules(1) informationFramework(1) }

    -- Selected object classes
        applicationEntity
        top
        ----
        FROM SelectedObjectClasses { joint-iso-ccitt
            ds(5) modules(1) selectedObjectClasses(6) }

    -- Selected attribute types
        commonName, description, distinguishedNameSyntax,
        integerSyntax, objectidentifierSyntax, organization,
        organizationalUnitName, owner, seeAlso
        ----
        FROM SelectedAttributeTypes { joint-iso-ccitt
            ds(5) modules(1) selectedAttributeTypes(5) }

-- OBJECT CLASSES

    -- MHS distribution list

        mhs-distribution-list OBJECT-CLASS
            SUBCLASS OF top
            MUST CONTAIN {
                  commonName,
                  mhs-dl-submit-permissions,
                  mhs-or-addresses }
            MAY CONTAIN {
                  description,
                  organization,
                  organizationalUnitName,
                  owner,
                  seeAlso,
                  mhs-deliverable-content-types,
                  mhs-deliverable-eits,
                  mhs-dl-members,
                  mhs-preferred-delivery-methods }
            :: id-oc-mhs-distribution-list

    -- MHS message store

        mhs-message-store OBJECT-CLASS
            SUB   CLASS OF applicationEntity
            MAY CONTAIN {
                  description,
                  owner,
                  mhs-supported-optional-attributes,
                  mhs-supported-automatic-actions,
                  mhs-supported-content-types }
            ::= id-oc-mhs-message-store

    -- MHS message transfer agent
        mhs-message-transfer-agent OBJECT-CLASS
            SUBCLASS OF applicationEntity
            MAY CONTAIN {
                  description,
                  owner,
                  mhs-deliverable-content-length }
            ::= id-oc-mhs-message-transfer-agent
    -- MHS user
        mhs-user OBJECT-CLASS
            SUBCLASS OF top
            MUST CONTAIN {
                mhs-or-addresses }
            MAY CONTAIN {
                mhs-deliverable-content-length,

                mhs-deliverable-content-types,
                mhs-deliverable-eits,
                mhs-message-store,
                mhs-preferred-delivery-methods }
            ::= id-oc-mhs-user

    -- MHS user agent
        mhs-user-agent OBJECT-CLASS
            SUBCLASS OF applicationEntity
            MAY CONTAIN {
                owner,
                mhs-deliverable-content-length,
                mhs-deliverable-content-types,
                mhs-deliverable-eits,
                mhs-or-addresses }
            ::= id-oc-mhs-user-agent

-- ATTRIBUTES

    -- MHS deliverable content length
        mhs-deliverable-content-length ATTRIBUTE
            WITH ATTRIBUTE-SYNTAX integerSyntax
            SINGLE VALUE
            ::= id-at-mhs-deliverable-content-length

    -- MHS deliverable content types
        mhs-deliverable-content-types ATTRIBUTE
            WITH ATTRIBUTE-SYNTAX objectIdentifierSyntax
            MULTI VALUE
            ::= id-at-mhs-deliverable-content-types

    -- MHS deliverable EITs
        mhs-deliverable-eits ATTRIBUTE
            WITH ATTRIBUTE-SYNTAX objectIdentifierSyntax
            MULTI VALUE
            ::= id-at-mhs-deliverable-eits

    -- MHS DL members
        mhs-dl-members ATTRIBUTE
            WITH ATTRIBUTE-SYNTAX mhs-or-name-syntax
            MULTI VALUE
            ::= id-at-mhs-dl-members

    -- MHS DL submit permissions
        mhs-dl-submit-permissions ATTRIBUTE
            WITH ATTRIBUTE-SYNTAX mhs-dl-submit-permission-syntax
            MULTI VALUE
            ::= id-at-mhs-dl-submit-permissions

    -- MHS O/R adresses
        mhs-or-addresses ATTRIBUTE
            WITH ATTRIBUTE-SYNTAX mhs-or-address-syntax
            MULTI VALUE
            ::= id-at-mhs-or-addresses

    -- MHS message store
```

```
                mhs-message-store ATTRIBUTE
                    WITH ATTRIBUTE-SYNTAX distinguishedNameSyntax
                    SINGLE VALUE
                    ::= id-at-mhs-message-store

        -- MHS preferred delivery methods
                mhs-preferred-delivery-methods ATTRIBUTE
                    WITH ATTRIBUTE-SYNTAX RequestedDeliveryMethod
                    MATCHES FOR EQUALITY
                    SINGLE VALUE
                    ::= id-at-mhs-preferred-delivery-methods

        -- MHS supported automatic actions
                mhs-supported-automatic-actions ATTRIBUTE
                    WITH ATTRIBUTE-SYNTAX objectIdentifierSyntax
                    MULTI VALUE
                    ::= id-at-mhs-supported-automatic-actions

        -- MHS supported content types
                mhs-suppported-content-types ATTRIBUTE
                    WITH ATTRIBUTE-SYNTAX objectIdentifierSyntax
                    MULTI VALUE
                    ::= id-at-mhs-supported-content-types

        -- MHS supported optional attributes
                mhs-supported-optional-attributes ATTRIBUTE
                    WITH ATTRIBUTE-SYNTAX objectIdentifierSyntax
                    MULTI VALUE
                    ::= id-at-mhs-supported-optional-attributes

-- ATTRIBUTE SYNTAXES

        -- MHS DL submit permission
                mhs-dl-submit-permission-syntax ATTRIBUTE-SYNTAX
                    SYNTAX DLSubmitPermission
                    MATCHES FOR EQUALITY
                    ::= id-as-mhs-dl-submit-permission

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

        -- MHS O/R addresses
                mhs-or-address-syntax ATTRIBUTE-SYNTAX
                    SYNTAX ORAddress
                    MATCHES FOR EQUALITY
                    ::= id-as-mhs-or-address

        -- MHS O/R name
                mhs-or-name-syntax ATTRIBUTE-SYNTAX
                    SYNTAX ORName
                    MATCHES FOR EQUALITY
                    ::= id-as-mhs-or-name

END -- of MHSdirectory
```

ANNEX D

Security threats

This Annex is not a part of this Recommendation.

An overview of MHS security threats is provided in § 15.1 of Recommendation X.400. This considers threats as they appear in an MHS access threats, inter-message threats, and message store threats. These threats can appear in various forms as follows:

a) masquerade;

b) message sequencing;

c) modification of information;

d) denial of service;

e) leakage of information;

f) repudiation;

g) other MHS threats.

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

Table D-1/X.402 indicates how these threats can be met using the MHS security services. The list of threats given here is indicative rather than definitive.

TABLE D-1/X.402

Use of MHS security services

Threat	Services
Masquerade	
Impersonation and misuse of the MTS	Message origin authentication
	Probe origin authentication
	Secure access management
Falsely acknowledge receipt	Proof of delivery
Falsely claim to originate a message	Message origin authentication
Impersonation of an MTA to an MTS-user	Proof of submission
	Report origin authentication
	Secure access management
Impersonation of an MTA to another MTA	Report origin authentication
	Secure access management
Message sequencing	
Replay of messages	Message sequence integrity
Re-ordering of messages	Message sequence integrity
Pre-play of messages	
Delay of messages	
Modification of information	
Modification of messages	Connection integrity
	Content integrity
Destruction of messages	Message sequence integrity
Corruption of routing and other management information	
Denial of service	
Denial of communications	
MTA flooding	
MTS flooding	
Repudiation	
Denial of origin	Non-repudiation of origin
Denial of submission	Non-repudiation of submission
Denial of delivery	Non-repudiation of delivery
Leakage of information	
Loss of confidentiality	Connection confidentiality
	Content confidentiality
Loss of anonymity	Message flow confidentiality
Misappropriation of messages	Secure access management
Traffic analysis	Message flow confidentiality
Other threats	
Originator not cleared for message security label	Secure access management
	Message security labelling
MTA/MTS-user not cleared for security context	Secure access management
Misrouting	Secure access management
	Message security labelling
Differing labelling policies	

D.1 *Masquerade*

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

Masquerade threats include the following:

a) impersonation and misuse of the MTS;

b) falsely acknowledge receipt;

c) falsely claim to originate a message;

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

e) impersonation of an MTA to another MTA.

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

D.2 *Message sequencing*

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

Message sequencing threats include the following:

a) replay of messages;

b) reordering of messages;

c) pre-play of messages;

d) delay of messages.

D.3 *Modification of information*

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

Modification of information threats include the following:

a) modification of messages;

b) destruction of messages;

c) corruption of routing and other management information.

D.4 *Denial of service*

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

Denial of service threats include the following:

a) denial of communications;

b) MTA failure;

c) MTS flooding.

D.5 *Repudiation*

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

Repudiation threats include the following:

a) denial of origin;

b) denial of submission;

c) denial of delivery.

D.6 *Leakage of information*

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

Leakage of information threats include the following:

a) loss of confidentiality;

b) loss of anonymity;

c) misappropriation of messages;

d) traffic analysis.

D.7 *Other threats*

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

Other threats include the following:

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

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

c) misrouting;

d) differing labelling policies.

ANNEX E

(to Recommendation X.402)

Provision of security services in Recommendation X.411

This Annex is an integral part of this Recommendation.

Table E-1/X.402 indicates which service elements from Recommendation X.411 may be used to support the security services described in § 10.2.

TABLE E-1/X.402

MHS security service provision

Service	MIS Arguments/services
Origin authentication security services	
Message origin authentication	Message origin authentication check
	Message token
Probe origin authentication	Probe origin authentication check
Report origin authentication	Report origin authentication check
Proof of submission	Proof of submission request
	Proof of submission
Proof of delivery	Proof of delivery request
	Proof of delivery
Secure access management security services	
Peer entity authentication	Initiator credentials
	Responder credentials
Security context	Security context
Data confidentiality security services	
Connection confidentiality	Not supported
Content confidentiality	Content confidentiality algorithm identifier
	Message token
Message flow confidentiality	Content type
Data integrity security services	
Connection integrity	Not supported
Content integrity	Content integrity check
	Message token
	Message origin authentication check
Message sequence integrity	Message sequence number
	Message token
Non-repudiation security services	
Non-repudiation of origin	Content integrity check
	Message token
	Message origin authentication check
Non-repudiation of submission	Proof of submission request
	Proof of submission
Non-repudiation of delivery	Proof of delivery request
	Proof of delivery
Message security labelling	Message security label
	Message token
	Message origin authentication check
Security management security services	
Change credentials	Change credentials
Register	Register

ANNEX F

Differences between CCITT Recommendation and ISO Standard

This Annex is not a part of this Recommendation.

This Annex lists all but the purely stylistic differences between this Recommendation and the corresponding ISO International Standard.

The following are the differences that exist:

a) The ISO International Standard corresponding to this Recommendation depicts direct connection of two PRMDs in the same country, direct connection of two PRMDs in different countries, and a single PRMD connected to two ADMDs, while this Recommendation does not. (See Figure 11/X.402.)

b) The ISO International Standard corresponding to this Recommendation does not require that ADMDs and PRMDs be hierarchically related for purposes of addressing and routing, while this Recommendation does. (See §§ 14.1.1., 14.1.2, 15 and 19.)

c) Where an O/R address attribute admits both printable and teletex strings, the ISO International Standard corresponding to this Recommendation does not require that the printable string be supplies as a minimum whenever attributes are conveyed internationally, while this Recommendation does. (See § 18.2.)

ANNEX G

Index

This Annex is not a part of this Recommendation.

This Annex indexes this Recommendation. It gives the number(s) of the section(s) on which each item in each of several categories is defined. Its coverage of each category is exhaustive.

This Annex indexes items (if any) in the following categories:

a) abbreviations;

b) terms;

c) information items;

d) ASN.1 modules;

e) ASN.1 macros;

f) ASN.1 types;

g) ASN.1 values;

h) *bilateral agreements*;

i) items **for further study**;

j) items **to be supplied (fs)**.

G.1 *Abbreviations*

G.2 *Terms*

ITU-T RECOMMENDATIONS SERIES

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

Printed in Switzerland
Geneva, 2008