



INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.411

(06/1999)

SERIES X: DATA NETWORKS AND OPEN SYSTEM
COMMUNICATIONS

Message Handling Systems

**Information technology – Message Handling
Systems (MHS) – Message Transfer System:
Abstract Service Definition and Procedures**

ITU-T Recommendation X.411

ITU-T X-SERIES RECOMMENDATIONS
DATA NETWORKS AND OPEN SYSTEM COMMUNICATIONS

PUBLIC DATA NETWORKS	
Services and facilities	X.1–X.19
Interfaces	X.20–X.49
Transmission, signalling and switching	X.50–X.89
Network aspects	X.90–X.149
Maintenance	X.150–X.179
Administrative arrangements	X.180–X.199
OPEN SYSTEMS INTERCONNECTION	
Model and notation	X.200–X.209
Service definitions	X.210–X.219
Connection-mode protocol specifications	X.220–X.229
Connectionless-mode protocol specifications	X.230–X.239
PICS proformas	X.240–X.259
Protocol Identification	X.260–X.269
Security Protocols	X.270–X.279
Layer Managed Objects	X.280–X.289
Conformance testing	X.290–X.299
INTERWORKING BETWEEN NETWORKS	
General	X.300–X.349
Satellite data transmission systems	X.350–X.369
IP-based networks	X.370–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	
Networking	X.600–X.629
Efficiency	X.630–X.639
Quality of service	X.640–X.649
Naming, Addressing and Registration	X.650–X.679
Abstract Syntax Notation One (ASN.1)	X.680–X.699
OSI MANAGEMENT	
Systems Management framework and architecture	X.700–X.709
Management Communication Service and Protocol	X.710–X.719
Structure of Management Information	X.720–X.729
Management functions and ODMA functions	X.730–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	
Commitment, Concurrency and Recovery	X.850–X.859
Transaction processing	X.860–X.879
Remote operations	X.880–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999

For further details, please refer to the list of ITU-T Recommendations.

**Information technology – Message Handling Systems (MHS) – Message Transfer System:
Abstract Service Definition and Procedures**

Summary

This Recommendation | International Standard contains an improved version of the P3 Register operation which introduces support for the Restricted Delivery element of service and adds general extensibility to the Register operation. The ASN.1 has been fully revised to use the new Recommendations X.680 and X.880, while retaining complete compatibility with the 1988 and 1992 P1 and P3 protocols. This Recommendation | International Standard incorporates enhancements on use of ISO/IEC 10646 characters in OR-addresses, new values of error codes for security and security defect resolution, using Version 3 certificates, business class messaging extensions, fax cover page, and use of 1997 Directory.

Source

The ITU-T Recommendation X.411 was approved on the 18 June 1999. The identical text is also published as ISO/IEC International Standard 10021-4.

Following ITU-T decision to publish new editions of the set of Message Handling Recommendations, this edition of ITU-T Rec. X.411 consolidates X.411 (11/1995), X.411 Technical Corrigendum 1 (08/1997), X.411 Amendment 1 (12/1997), X.411 Technical Corrigendum 2 (12/1997) and X.411 Technical Corrigendum 3 (09/1998).

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Conference (WTSC), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSC Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

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

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU [had/had not] received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

© ITU 2003

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

CONTENTS

Page

SECTION ONE – INTRODUCTION	1
1 Scope	1
2 Normative references	1
2.1 Open Systems Interconnection	2
2.2 Message Handling Systems	2
2.3 Directory Systems	2
2.4 Country Codes	3
2.5 Telematic Services	3
3 Definitions	3
4 Abbreviations	3
5 Conventions	3
5.1 Terms	3
5.2 Presence of Parameters	3
5.3 Abstract Syntax Definitions	3
5.4 Interpretation of UTC Time values	4
SECTION TWO – MESSAGE TRANSFER SYSTEM ABSTRACT SERVICE	4
6 Message Transfer System Model	4
7 Message Transfer System Abstract Service Overview	5
MTS Bind and Unbind	5
Submission Port Abstract Operations	5
Delivery Port Abstract Operations	5
Administration Port Abstract Operations	6
7.1 MTS Bind and Unbind	6
7.2 Submission Port	6
7.3 Delivery Port	6
7.4 Administration Port	6
8 Message Transfer System Abstract Service Definition	6
8.1 MTS-bind and MTS-unbind	6
8.1.1 Abstract-bind and Abstract-unbind	7
8.1.2 Bind-errors	10
8.2 Submission Port	10
8.2.1 Abstract-operations	10
8.2.2 Abstract-errors	31
8.3 Delivery Port	33
8.3.1 Abstract-operations	33
8.3.2 Abstract-errors	48
8.4 Administration Port	50
8.4.1 Abstract-operations	50
8.4.2 Abstract-errors	55
8.5 Common Parameter Types	56
8.5.1 MTS-identifier	56
8.5.2 Global-domain-identifier	57
8.5.3 MTA-name	57
8.5.4 Time	57
8.5.5 OR-name	57
8.5.6 Encoded-information-types	57
8.5.7 Certificate	58
8.5.8 Token	60
8.5.9 Security-label	60
8.5.10 Algorithm-identifier	61
8.5.11 Password	61
9 Message Transfer System Abstract Syntax Definition	61
9.1 Extension Mechanism	62
9.2 Criticality Mechanism	62

SECTION THREE – MESSAGE TRANSFER AGENT ABSTRACT SERVICE	102
10 Refined Message Transfer System Model	102
11 Message Transfer Agent Abstract Service Overview	103
MTA-bind and MTA-unbind	103
Transfer Port Abstract-operations	103
11.1 MTA-bind and MTA-unbind	103
11.2 Transfer Port Abstract-operations	103
12 Message Transfer Agent Abstract Service Definition	103
12.1 MTA-bind and MTA-unbind	103
12.1.1 Abstract-bind and Abstract-unbind	104
12.1.2 Bind-errors	106
12.2 Transfer Port	107
12.2.1 Abstract-operations	107
12.2.2 Abstract-errors	113
12.3 Common Parameter Types	113
12.3.1 Trace-information and internal-trace-information	113
13 Message Transfer Agent Abstract Syntax Definition	115
SECTION FOUR – PROCEDURES FOR DISTRIBUTED OPERATION OF THE MTS	123
14 Procedures for Distributed Operation of the MTS	123
14.1 Overview of the MTA Model	123
14.1.1 Organization and Modelling Technique	123
14.2 Deferred Delivery Module	125
14.2.1 Deferred Delivery Procedure	125
14.3 Main Module	126
14.3.1 Control Procedure	128
14.3.2 Front-end Procedure	130
14.3.3 Routing-and-conversion-decision Procedure	131
14.3.4 Routing-decision Procedure	132
14.3.5 Conversion-decision Procedure	134
14.3.6 Error-processing Procedure	135
14.3.7 Redirection Procedure	136
14.3.8 Splitter Procedure	137
14.3.9 Conversion-procedure	138
14.3.10 Distribution-list-expansion Procedure	138
14.3.11 Loop Detection and Routing Algorithm	140
14.3.12 Directory Name Resolution Procedure	140
14.3.13 Double-enveloper Procedure	141
14.3.14 Double-envelope-extractor Procedure	142
14.4 Report Module	143
14.4.1 Control Procedure	143
14.4.2 Report-front-end Procedure	144
14.4.3 Report-generation Procedure	144
14.4.4 Report-routing Procedure	145
14.4.5 Double-enveloper Procedure	147
14.5 MTS-bind and MTS-unbind	147
14.5.1 MTS-user initiated MTS-bind Procedure	147
14.5.2 MTS-user initiated MTS-unbind Procedure	148
14.5.3 MTA initiated MTS-bind Procedure	148
14.5.4 MTA initiated MTS-unbind Procedure	149
14.6 Submission Port	149
14.6.1 Message-submission Procedure	149
14.6.2 Probe-submission Procedure	150
14.6.3 Cancel-deferred-delivery Procedure	151
14.6.4 Submission-control Procedure	152
14.7 Delivery Port	152
14.7.1 Message-delivery Procedure	152
14.7.2 Probe-delivery-test Procedure	154

	<i>Page</i>
14.7.3 Report-delivery Procedure	155
14.7.4 Delivery-control Procedure	155
14.8 Administration Port	156
14.8.1 Register Procedure	156
14.8.2 MTS-user initiated Change-credentials Procedure	157
14.8.3 MTA initiated Change-credentials Procedure	157
14.9 MTA-bind and MTA-unbind	158
14.9.1 MTA-bind-in Procedure	158
14.9.2 MTA-unbind-in Procedure	158
14.9.3 MTA-bind-out Procedure	159
14.9.4 MTA-unbind-out Procedure	159
14.10 Transfer Port	160
14.10.1 Message-in Procedure	160
14.10.2 Probe-in Procedure	160
14.10.3 Report-in Procedure	161
14.10.4 Message-out Procedure	161
14.10.5 Probe-out Procedure	162
14.10.6 Report-out Procedure	162
Annex A – Reference Definition of MTS Object Identifiers	164
Annex B – Reference Definition of MTS Parameter Upper Bounds	166
Annex C – Definition of 1988 Message Transfer System Abstract Service	169
C.1 Register-88	169
C.1.1 Arguments	169
C.1.2 Results	170
C.1.3 Abstract-errors	170
C.2 Delivery-control-88	171
C.2.1 Arguments	171
C.2.2 Results	171
C.2.3 Abstract-errors	171
Annex D – Differences between ISO/IEC 10021-4 and ITU-T Recommendation X.411	175
Annex E – Index	176

Introduction

This Service Definition is one of a set of Recommendations | International Standards defining Message Handling in a distributed open systems environment.

Message Handling provides for the exchange of messages between users on a store-and-forward basis. A message submitted by one user (the *originator*) is transferred through the Message Transfer System (MTS) and delivered to one or more other users (the *recipients*).

The MTS comprises a number of message-transfer-agents (MTAs), which transfer messages and deliver them to their intended recipients.

This Service Definition was developed jointly by ITU-T and ISO/IEC. It is published as common text as ITU-T Rec. X.411 | ISO/IEC 10021-4.

.....

**INTERNATIONAL STANDARD ISO/IEC 10021-4
ITU-T RECOMMENDATION X.411**

**Information Technology – Message Handling Systems (Mhs) – Message Transfer System:
Abstract Service Definition And Procedures**

SECTION ONE – INTRODUCTION

1 Scope

This Recommendation | International Standard defines the abstract-service provided by the MTS (the MTS Abstract Service), and specifies the procedures to be performed by MTAs to ensure the correct distributed operation of the MTS.

ITU-T Rec. X.402 | ISO/IEC 10021-2 identifies the other Recommendations | International Standards which define other aspects of Message Handling Systems.

Access to the MTS Abstract Service defined in this Recommendation | International Standard may be provided by the MTS Access Protocol (P3) defined in ITU-T Rec. X.419 | ISO/IEC 10021-6. The distributed operation of the MTS defined in this Recommendation | International Standard may be provided by the use of the MTS Transfer Protocol (P1) also defined in ITU-T Rec. X.419 | ISO/IEC 10021-6. The means by which messages may be routed through the MTS is specified in ISO/IEC 10021-10.

Section two of this Recommendation | International Standard defines the MTS Abstract Service. Clause 6 describes the Message Transfer System Model. Clause 7 provides an overview of the MTS Abstract Service. Clause 8 defines the semantics of the parameters of the MTS Abstract Service. Clause 9 defines the abstract-syntax of the MTS Abstract Service.

Section three of this Recommendation | International Standard defines the MTA Abstract Service. Clause 10 refines the model of the MTS, first presented in clause 6, to show that the MTS comprises a number of MTAs that interwork with one another to provide the MTS Abstract Service. Clause 11 provides an overview of the MTA Abstract Service. Clause 12 defines the semantics of the parameters of the MTA Abstract Service. Clause 13 defines the abstract-syntax of the MTA Abstract Service.

Section four of this Recommendation | International Standard specifies the procedures performed by MTAs to ensure the correct distributed operation of the MTS.

Annex A provides a reference definition of the MTS object identifiers cited in the ASN.1 modules in the body of this Recommendation | International Standard.

Annex B provides a reference definition of the upper bounds of the size constraints imposed upon variable length data types defined in ASN.1 modules in ITU-T Rec. X.411.

Annex C identifies the technical differences between the ISO/IEC and ITU-T versions of ITU-T Rec. X.411 and ISO/IEC 10021-4.

Annex D provides an index to this Recommendation | International Standard, categorised into: definitions of the MTS parameters; Abbreviations; Terms; ASN.1 modules; ASN.1 information object classes; ASN.1 types; and ASN.1 values.

2 Normative references

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

2.1 Open Systems Interconnection

This Service Definition cites the following OSI specifications:

- ITU-T Recommendation X.680 (1997) | ISO/IEC 8824-1:1998, *Information technology – Abstract Syntax Notation One (ASN.1) – Specification of Basic Notation.*
- ITU-T Recommendation X.681 (1997) | ISO/IEC 8824-2:1998, *Information technology – Abstract Syntax Notation One (ASN.1) – Information Object Specification.*
- ITU-T Recommendation X.682 (1997) | ISO/IEC 8824-3:1998, *Information technology – Abstract Syntax Notation One (ASN.1) – Constraint Specification.*
- ITU-T Recommendation X.683 (1997) | ISO/IEC 8824-4:1998, *Information technology – Abstract Syntax Notation One (ASN.1) – Parameterization of ASN.1 Specifications.*
- ITU-T Recommendation X.880 (1994) | ISO/IEC 13712-1:1995, *Information technology – Remote Operations – Concepts, Model and Notation.*

2.2 Message Handling Systems

This Service Definition cites the following Message Handling System specifications:

- ITU-T Recommendation F.400/X.400 (1999), *Message handling: System and service overview.*
ISO/IEC 10021-1:1999, *Information technology – Message Handling Systems (MHS) – Part 1: System and service overview.*
- ITU-T Recommendation X.402 (1999) | ISO/IEC 10021-2:1999, *Information technology – Message Handling Systems (MHS) – Overall architecture.*
- ITU-T Recommendation X.413 (1999) | ISO/IEC 10021-5:1999, *Information technology – Message Handling Systems (MHS) – Message store: Abstract service definition.*
- ITU-T Recommendation X.419 (1999) | ISO/IEC 10021-6:1999, *Information technology – Message Handling Systems (MHS) – Protocol specifications.*
- ITU-T Recommendation X.420 (1999) | ISO/IEC 10021-7:1999, *Information technology – Message Handling Systems (MHS) – Interpersonal messaging system.*
- ITU-T Recommendation X.412 (1999) | ISO/IEC 10021-10:1999, *Information technology – Message Handling Systems (MHS) – MHS Routing.*
- CCITT Recommendation X.408 (1988), *Message handling systems: Encoded information type conversion rules.*

2.3 Directory Systems

This Service Definition cites the following Directory System specifications:

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

- ITU-T Recommendation X.530 (1997) | ISO/IEC 9594-10:1998, *Information Technology – Open Systems Interconnection – The Directory: Use of systems management for administration of the Directory*.

2.4 Country Codes

This Service Definition cites the following Country Code specifications:

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

2.5 Telematic Services

This Service Definition cites the following Telematic Service specifications:

- CCITT Recommendation F.170 (1992), *Operational provisions for the international public facsimile service between public bureaux (bureaufax)*.
- ITU-T Recommendation T.30 (1993), *Procedures for document facsimile transmission in the general switched telephone network*.

3 Definitions

For the purposes of this Service Definition the definitions given in ITU-T Rec. X.402 | ISO/IEC 10021-2 apply.

4 Abbreviations

For the purposes of this Service Definition the abbreviations given in ITU-T Rec. X.402 | ISO/IEC 10021-2 apply.

5 Conventions

This Service Definition uses the descriptive conventions described below.

5.1 Terms

Throughout this Service Definition the words of defined terms and the names and values of the parameters of the MTS Abstract Service and the MTA Abstract Service, unless they are proper names, begin with a lower-case letter and are linked by a hyphen thus: defined-term. Proper names begin with an upper-case letter and are not linked by a hyphen thus: Proper Name. The names and values of the parameters of the MTS Abstract Service and the MTA Abstract Service (including components of OR address defined in ISO/IEC 10021-2) are printed in **bold**.

5.2 Presence of Parameters

In the tables of parameters in clauses 8 and 12, the presence of each parameter is qualified as follows:

Mandatory (M): A mandatory parameter shall always be present.

Optional (O): An optional argument shall be present at the discretion of the invoker of the abstract-operation; an optional result shall be present at the discretion of the performer of the abstract-operation.

Conditional (C): A conditional parameter shall be present under the circumstances prescribed by this Service Definition.

Where a conditional parameter shall be present due to some action on the message, probe or report by the MTS, this is explicitly defined. The presence of other conditional parameters is dependent on the presence of those parameters in other abstract-operations (for example, the presence of a conditional argument of the Message-transfer abstract-operation is dependent on the presence of the same optional argument in the related Message-submission abstract-operation).

5.3 Abstract Syntax Definitions

This Service Definition defines the abstract-syntax of the MTS Abstract Service and the MTA Abstract Service using the abstract syntax notation (ASN.1) defined in ITU-T Rec. X.680 | ISO/IEC 8824-1, ITU-T Rec. X.681 |

ISO/IEC 8824-2, ITU-T Rec. X.682 | ISO/IEC 8824-3 and ITU-T Rec. X.683 | ISO/IEC 8824-4, and the abstract service definition conventions described in ITU-T Rec. X.402 | ISO/IEC 10021-2 which use the remote operations notation defined in ITU-T Rec. X.880 | ISO/IEC 13712-1.

Where there are changes implied to the protocols defined in CCITT Recommendation X.411 (1984), these are highlighted in the abstract syntax definitions by means of underlining.

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

5.4 Interpretation of UTC Time values

Dates and times in the MHS protocols are represented using the ASN.1 *UTCTime* type which uses only two decimal digits to represent the year, leaving the century unspecified. Since MHS systems must deal with dates both in the past (e.g. submission times of old messages which may be held in local storage or forwarded) and in the future (expiry time, deferred delivery time), it is important to observe a standard convention to avoid inaccurate display or malfunction of the MHS when dates from different centuries are compared.

The two decimal digits give 100 different years that can be expressed; an implementation has to associate each of these values with a particular century. The chosen convention is that dates up to ten years prior to the current time and up to forty years ahead of the current time should be associated with the corresponding century, with the interpretation of the remaining 49 values being implementation dependent. For example, for a system operating in 1996 the values "86" to "99" are interpreted as 1986 to 1999 and the values "00" to "36" are interpreted as 2000 to 2036, and the values "37" to "85" are implementation dependent.

NOTE – This convention permits two possible implementation strategies. An implementation can choose a fixed interpretation of all the year values, such that the convention is satisfied throughout the expected life of the product, or it can interpret the dates dynamically, based on the current date, such that the implementation remains valid indefinitely. For example, an implementation could choose the fixed range 1970 to 2069 for the available values, meaning that the implementation would require revision if it is still in use by the year 2029.

SECTION TWO – MESSAGE TRANSFER SYSTEM ABSTRACT SERVICE

6 Message Transfer System Model

Message Handling provides for the exchange of messages between users on a store-and-forward basis. A message submitted by one user (the *originator*) is transferred through the Message Transfer System (MTS) and delivered to one or more other users (the *recipients*).

The MTS is described using an abstract model in order to define the services provided by the MTS as a whole – the MTS Abstract Service.

The MTS is modelled as an *object*, whose overall behaviour can be described without reference to its internal structure. The services provided by the MTS object are made available at *ports*. A type of port represents a particular view of the services provided by the MTS object.

A user of the MTS is also modelled as an object, which obtains the services provided by the MTS through a port which is paired with an MTS port of the same type.

A type of port corresponds to a set of *abstract-operations* which can occur at the port; those which can be performed by the MTS object (invoked by the MTS-user object), and those which can be invoked by the MTS object (performed by the MTS-user object).

A port may be symmetrical, in which case the set of operations performed by the MTS object may also be invoked by the MTS object, and vice versa. Otherwise, the port is asymmetrical, in which case the object is said to be the *supplier* or *consumer* with respect to the type of port. The terms *supplier* and *consumer* are used only to distinguish between the roles of a pair of ports in invoking or performing operations. The assignment of the terms is usually intuitive when one object is providing a service used by another object; the service object (e.g., the MTS) is usually regarded as being the *supplier*, and the user object (e.g., an MTS-user object) is usually regarded as being the *consumer*.

Before objects can invoke operations on one another, they must be bound into an abstract *association*. The binding of an association between objects establishes a relationship between the objects which lasts until the association is released. An association is always released by the initiator of the association. The binding of an association establishes the *credentials* of the objects to interact, and the *application-context* and *security-context* of the association. The *application-context* of an association may be one or more types of port paired between the two objects.

The model presented is abstract. That is, it is not always possible for an outside observer to identify the boundaries between objects, or to decide on the moment or the means by which operations occur. However, in some cases the abstract model will be *realised*. For example, a pair of objects which communicate through paired ports may be located in different open systems. In this case, the boundary between the objects is visible, the ports are exposed, and the operations may be supported by instances of OSI communication.

The MTS object supports ports of three different types: a *submission-port*, a *delivery-port* and an *administration-port*.

A submission-port enables an MTS-user to submit messages to the MTS for transfer and delivery to one or more recipient MTS-users, and to probe the ability of the MTS to deliver a subject-message.

A delivery-port enables an MTS-user to accept delivery of messages from the MTS, and to accept reports on the delivery or non-delivery of messages and probes.

An administration-port enables an MTS-user to change long term parameters held by the MTS associated with message delivery, and enables either the MTS or the MTS-user to change their *credentials* with one another.

A message submitted by one MTS-user via a submission-port will normally be delivered to one or more recipient MTS-users via delivery-ports. The originating MTS-user may elect to be notified of the delivery or non-delivery of a message via its delivery-port.

Figure 1 models the Message Transfer System (MTS).

Clause 7 provides an overview of the MTS Abstract Service.

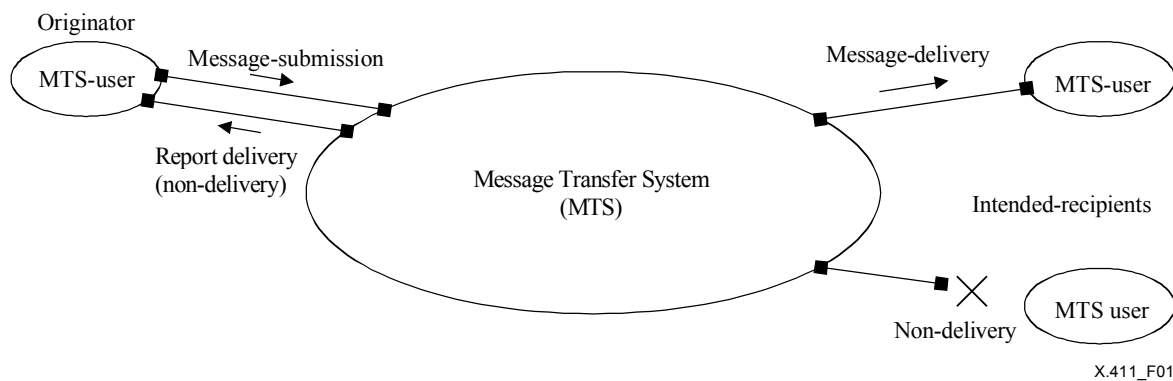


Figure 1 – Message Transfer System Model

7 Message Transfer System Abstract Service Overview

This Service Definition defines the following services that comprise the MTS Abstract Service:

MTS Bind and Unbind

- a) MTS-bind
- b) MTS-unbind

Submission Port Abstract Operations

- c) Message-submission
- d) Probe-submission
- e) Cancel-deferred-delivery
- f) Submission-control

Delivery Port Abstract Operations

- g) Message-delivery
- h) Report-delivery
- i) Delivery-control

Administration Port Abstract Operations

- j) Register
- k) Change-credentials.

7.1 MTS Bind and Unbind

The **MTS-bind** enables either the MTS-user to establish an association with the MTS, or the MTS to establish an association with the MTS-user. Abstract-operations other than MTS-bind can only be invoked in the context of an established association.

The **MTS-unbind** enables the release of an established association by the initiator of the association.

7.2 Submission Port

The **Message-submission** abstract-operation enables an MTS-user to submit a message to the MTS for transfer and delivery to one or more recipient MTS-users.

The **Probe-submission** abstract-operation enables an MTS-user to submit a probe in order to determine whether or not a message could be transferred and delivered to one or more recipient MTS-users if it were to be submitted.

The **Cancel-deferred-delivery** abstract-operation enables an MTS-user to request cancellation of a message previously submitted (for deferred-delivery) by invocation of the Message-submission abstract-operation.

The **Submission-control** abstract-operation enables the MTS to constrain the use of the submission-port abstract-operations by the MTS-user.

The **Message-submission** and **Probe-submission** abstract-operations may cause subsequent invocation of the Report-delivery abstract-operation by the MTS.

7.3 Delivery Port

The **Message-delivery** abstract-operation enables the MTS to deliver a message to an MTS-user.

The **Report-delivery** abstract-operation enables the MTS to acknowledge to the MTS-user the outcome of a previous invocation of the Message-submission or Probe-submission abstract-operations. For the Message-submission abstract-operation, the Report-delivery abstract-operation indicates the delivery or non-delivery of the submitted message. For the Probe-submission abstract-operation, the Report-delivery abstract-operation indicates whether or not a message could be delivered if it were to be submitted. The Report-delivery abstract-operation may also convey a notification of physical-delivery by a PDS.

The **Delivery-control** abstract-operation enables an MTS-user to constrain the use of the delivery-port abstract-operations by the MTS.

7.4 Administration Port

The **Register** abstract-operation enables an MTS-user to change long term parameters of the MTS-user held by the MTS, associated with message delivery.

The **Change-credentials** abstract-operation enables either an MTS-user to change its **credentials** with the MTS, or the MTS to change its **credentials** with the MTS-user.

8 Message Transfer System Abstract Service Definition

This clause defines the semantics of the parameters of the MTS Abstract Service.

Clause 8.1 defines the MTS-bind and MTS-unbind. Clause 8.2 defines the submission-port. Clause 8.3 defines the delivery-port. Clause 8.4 defines the administration-port. Clause 8.5 defines some common parameter types.

The abstract-syntax of the MTS Abstract Service is defined in clause 9.

8.1 MTS-bind and MTS-unbind

This clause defines the MTS-bind and MTS-unbind used to establish and release associations between an MTS-user and the MTS.

8.1.1 Abstract-bind and Abstract-unbind

This clause defines the following abstract-bind and abstract-unbind operations:

- a) MTS-bind
- b) MTS-unbind.

8.1.1.1 MTS-bind

The MTS-bind enables an MTS-user to establish an association with the MTS, or the MTS to establish an association with an MTS-user.

The MTS-bind establishes the **credentials** of an MTS-user and the MTS to interact, and the **application-context** and security-context of the association. An association can only be released by the initiator of that association (using MTS-unbind).

Abstract-operations other than MTS-bind can only be invoked in the context of an established association.

The successful completion of the MTS-bind signifies the establishment of an association.

The disruption of the MTS-bind by a bind-error indicates that an association has not been established.

8.1.1.1.1 Arguments

Table 1 lists the arguments of the MTS-bind, and for each argument qualifies its presence and indicates the clause in which the argument is defined.

Table 1 – MTS-bind Arguments

Argument	Presence	Clause
<i>Bind Arguments</i>		
Initiator-name	M	8.1.1.1.1.1
Initiator-credentials	M	8.1.1.1.1.2
Security-context	O	8.1.1.1.1.3
Messages-waiting	O	8.1.1.1.1.4

8.1.1.1.1.1 Initiator-name

This argument contains a name for the initiator of the association. It shall be generated by the initiator of the association.

If the initiator is an MTS-user, the name is the **OR-name** of the MTS-user, which is registered with the MTS (see 8.4.1.1.1.1). The **initiator-name** shall contain the **OR-address**, and may optionally also contain the **directory-name**, of the MTS-user (**OR-address-and-optional-directory-name**). The **initiator-name** shall also indicate whether the initiator is a UA or an MS.

If the initiator is the MTS (or an MTA – see clause 11), the name is an **MTA-name**, which is known to the MTS-user.

8.1.1.1.1.2 Initiator-credentials

This argument contains the **credentials** of the initiator of the association. It shall be generated by the initiator of the association.

The **initiator-credentials** may be used by the responder to authenticate the identity of the initiator (see ITU-T Rec. X.509 | ISO/IEC 9594-8).

If only simple-authentication is used, the **initiator-credentials** comprise a simple **password** associated with the **initiator-name**.

If protected-authentication is used, the **initiator-credentials** comprise a **password** protected as described in clause 6 of ITU-T Rec. X. 509 | ISO/IEC 9594-8 (either Protected1 or Protected2) and optionally arguments for that protection process (time1, time2, random1 and random2) which derive their meaning by bilateral agreement. The description of protected-authentication in Annex H of ITU-T Rec. X.402 | ISO/IEC 10021-2 applies equally to MTS-bind (apart from the protected mechanism to change the password).

If strong-authentication is used, the **initiator-credentials** comprise an **initiator-bind-token** and, optionally, an **initiator-certificate** or **certificate-selector**.

The **initiator-bind-token** is a **token** generated by the initiator of the association. If the **initiator-bind-token** is an **asymmetric-token**, the **signed-data** comprises a **random-number**. The **encrypted-data** of an **asymmetric-token** may be used to convey secret security-relevant information (e.g., one or more symmetric-encryption-keys) used to secure the association, or may be absent from the **initiator-bind-token**.

Symmetric algorithms may be used within the above **asymmetric-token** (see 8.5.8).

The **initiator-certificate** is a **certificate** of the initiator of the association, generated by a trusted source (e.g., a certification-authority), and, optionally, additional certificates which provide a certification-path for the initiator's certificate. It may be supplied by the initiator of the association, if the **initiator-bind-token** is an **asymmetric-token**. If the initiator is an MTS-user, the **initiator-certificate** shall contain the **OR-address** of the initiator in the *x400Address* component in its subject alternative name field (see 12.3.2.1 of ITU-T Rec. X.509 | ISO/IEC 9594-8), unless the security-policy provides an alternative binding of the certificate to the MTS-user. If the initiator is the MTS, the **initiator-certificate** shall contain the **MTA-name** of the initiator in an *mta-name* (see A.5.1 of ITU-T Rec. X.402 | ISO/IEC 10021-2) in the *otherName* component in its subject alternative name field, unless the security-policy provides an alternative binding of the certificate to the initiating MTA. The **initiator-certificate** may be used to convey a verified copy of the public-asymmetric-encryption-key (**subject-public-key**) of the initiator of the association. The initiator's public-asymmetric-encryption-key may be used by the responder to validate the **initiator-bind-token** and to compute **encrypted-data** in the **responder-bind-token**. If the responder is known to have, or have access to, the initiator's **certificate** (e.g., via the Directory), the **initiator-certificate** may be omitted and, where the initiator has more than one certificate, a **certificate-selector** may be supplied to identify the certificate using any certificate selection criteria specified for certificate match (see 12.7.2 of ITU-T Rec. X.509 | ISO/IEC 9594-8).

8.1.1.1.3 Security-context

This argument identifies the **security-context** that the initiator of the association proposes to operate at. It may be generated by the initiator of the association.

The **security-context** comprises one or more **security-labels** that define the sensitivity of interactions that may occur between the MTS-user and the MTS for the duration of the association, in line with the security-policy in force. The **security-context** shall be one that is allowed by the registered **user-security-labels** of the MTS-user and by the **security-labels** associated with the MTA of the MTS.

Once established, the **security-context** of the submission-port and delivery-port can be temporarily restricted using the Submission-control (see 8.2.1.4.5) and Delivery-control (see 8.3.1.3.1.7) abstract-operations, respectively.

If **security-contexts** are not established between the MTS-user and the MTS, the sensitivity of interactions that may occur between the MTS-user and the MTS may be at the discretion of the invoker of an abstract-operation.

8.1.1.1.4 Messages-waiting

This argument indicates the number of messages and total number of octets waiting to be delivered by the MTS to the MTS-user, for each **priority**. It may be generated by the initiator of the association.

This argument shall only be present when the MTS is initiating an association with an MTS-user, and when the MTS-user subscribes to the Hold for Delivery element-of-service (defined in ITU-T Rec. X.400 | ISO/IEC 10021-1).

8.1.1.1.2 Results

Table 2 lists the results of the MTS-bind, and for each result qualifies its presence and indicates the clause in which the result is defined.

Table 2 – MTS-bind Results

Result	Presence	Clause
<i>Bind Results</i>		
Responder-name	M	8.1.1.1.2.1
Responder-credentials	M	8.1.1.1.2.2
Messages-waiting	O	8.1.1.1.2.3

8.1.1.1.2.1 Responder-name

This argument contains a name for the responder of the association. It shall be generated by the responder of the association.

If the responder is an MTS-user, the name is the **OR-name** of the MTS-user, which is registered with the MTS (see 8.4.1.1.1.1). The **responder-name** shall contain the **OR-address**, and may optionally also contain the **directory-name**, of the MTS-user (**OR-address-and-optional-directory-name**). The **responder-name** shall also indicate whether the responder is a UA or an MS.

If the responder is the MTS (or an MTA – see clause 11), the name is an **MTA-name**, which is known to the MTS-user.

8.1.1.1.2.2 Responder-credentials

This argument contains the **credentials** of the responder of the association. It shall be generated by the responder of the association.

The **responder-credentials** may be used by the initiator to authenticate the identity of the responder (see ITU-T Rec. X.509 | ISO/IEC 9594-8).

If only simple-authentication is used, the **responder-credentials** comprise a simple **password** associated with the **responder-name**.

If protected-authentication is used, the **responder-credentials** comprise a **password** protected as described in clause 6 of ITU-T Rec. X.509 | ISO/IEC 9594-8 (either Protected1 or Protected2) and optionally arguments for that protection process (time1, time2, random1 and random2) which derive their meaning by bilateral agreement.

If strong-authentication is used, the **responder-credentials** comprise a **responder-bind-token** and, optionally, a **responder-certificate** or **certificate-selector**. The **responder-bind-token** is a **token** generated by the responder of the association. The **responder-bind-token** shall be the same type of **token** as the **initiator-bind-token**. If the **responder-bind-token** is an **asymmetric-token**, the **signed-data** comprises a **random-number** (which may be related to the **random-number** supplied in the **initiator-bind-token**). The **encrypted-data** of an **asymmetric-token** may be used to convey secret security-relevant information (e.g., one or more symmetric-encryption-keys) used to secure the association, or may be absent from the **responder-bind-token**.

Symmetric algorithms may be used within the above **asymmetric-token** (see 8.5.8).

The **responder-certificate** is a **certificate** of the responder of the association, generated by a trusted source (e.g. a certification-authority) and, optionally, additional certificates which provide a certification-path for the responder's certificate. It may be supplied by the responder of the association, if the **responder-bind-token** is an **asymmetric-token**. If the responder is an MTS-user, the **responder-certificate** shall contain the **OR-address** of the responder in the *x400Address* component in its subject alternative name field (see 12.3.2.1 of ITU-T Rec. X.509 | ISO/IEC 9594-8), unless the security-policy provides an alternative binding of the certificate to the MTS-user. If the responder is the MTS, the **responder-certificate** shall contain the **MTA-name** of the responder in an *mta-name* (see A.5.1 of ITU-T Rec. X.402 | ISO/IEC 10021-2) in the *otherName* component in its subject alternative name field, unless the security-policy provides an alternative binding of the certificate to the responding MTA. The **responder-certificate** may be used to convey a verified copy of the public-asymmetric-encryption-key (**subject-public-key**) of the responder of the association. The responder's public-asymmetric-encryption-key may be used by the initiator to validate the **responder-bind-token**. If the initiator is known to have, or have access to, the responder's **certificate** (e.g. via the Directory), the **responder-certificate** may be omitted and, where the responder has more than one certificate, a **certificate-selector** may be supplied to identify the certificate using any certificate selection criteria specified for certificate match (see 12.7.2 of ITU-T Rec. X.509 | ISO/IEC 9594-8).

8.1.1.1.2.3 Messages-waiting

This argument indicates the number of messages and total number of octets waiting to be delivered by the MTS to the MTS-user, for each **priority**. It may be generated by the responder of the association.

This argument shall only be present when the MTS is responding to an association initiated by an MTS-user, and when the MTS-user subscribes to the Hold for Delivery element-of-service (defined in ITU-T Rec. X.400 | ISO/IEC 10021-1).

8.1.1.1.3 Bind-errors

The bind-errors that may disrupt the MTS-bind are defined in 8.1.2.

8.1.1.2 MTS-unbind

The MTS-unbind enables the release of an established association by the initiator of the association.

8.1.1.2.1 Arguments

The MTS-unbind has no arguments.

8.1.1.2.2 Results

The MTS-unbind returns an empty result as indication of release of the association.

8.1.1.2.3 Unbind-errors

There are no unbind-errors that may disrupt the MTS-unbind.

8.1.2 Bind-errors

This clause defines the following bind-errors:

- a) Authentication-error
- b) Busy
- c) Unacceptable-dialogue-mode
- d) Unacceptable-security-context
- e) Inadequate-association-confidentiality.

8.1.2.1 Authentication-error

The Authentication-error bind-error reports that an association cannot be established due to an authentication error; the initiator's **credentials** are not acceptable or are improperly specified.

The Authentication-error bind-error has no parameters.

8.1.2.2 Busy

The Busy bind-error reports that an association cannot be established because the responder is busy.

The Busy bind-error has no parameters.

8.1.2.3 Unacceptable-dialogue-mode

The Unacceptable-dialogue-mode bind-error reports that the dialogue-mode proposed by the initiator of the association is unacceptable to the responder (see ITU-T Rec. X.419 | ISO/IEC 10021-6).

The Unacceptable-dialogue-mode bind-error has no parameters.

8.1.2.4 Unacceptable-security-context

The Unacceptable-security-context bind-error reports that the **security-context** proposed by the initiator of the association is unacceptable to the responder.

The Unacceptable-security-context bind-error has no parameters.

8.1.2.5 Inadequate-association-confidentiality

The Inadequate-association-confidentiality bind-error reports that an association cannot be established because the underlying connection does not provide the necessary confidentiality.

8.2 Submission Port

This clause defines the abstract-operations and abstract-errors which occur at a submission-port.

8.2.1 Abstract-operations

This clause defines the following submission-port abstract-operations:

- a) Message-submission
- b) Probe-submission
- c) Cancel-deferred-delivery
- d) Submission-control.

8.2.1.1 Message-submission

The Message-submission abstract-operation enables an MTS-user to submit a message to the MTS for transfer and delivery to one or more recipient MTS-users.

The successful completion of the abstract-operation signifies that the MTS has accepted responsibility for the message (but not that it has yet delivered it to its intended recipients).

The disruption of the abstract-operation by an abstract-error indicates that the MTS cannot assume responsibility for the message.

8.2.1.1.1 Arguments

Table 3 lists the arguments of the Message-submission abstract-operation, and for each argument qualifies its presence and identifies the clause in which the argument is defined.

8.2.1.1.1.1 Originator-name

This argument contains the **OR-name** of the originator of the message. It shall be generated by the originating MTS-user. If **OR-address** is not included in **originator-name** on submission it shall be inserted by the originating MTA. The **originator-name** shall remain unchanged in the subsequent progress of the submitted message through the MTS. Where security arguments use the **originator-name**, its **OR-address** shall be generated by the originating MTS-user.

The **originator-name** contains the **OR-name** of an individual originator, i.e., it shall not contain the **OR-name** of a DL.

8.2.1.1.1.2 Recipient-name

This argument contains the **OR-name** of a recipient of the message. It shall be generated by the originator of the message. A value of this argument shall be specified for each recipient of the message.

The **recipient-name** contains the **OR-name** of an individual recipient or DL.

8.2.1.1.1.3 Alternate-recipient-allowed

This argument indicates whether the message may be delivered to an alternate-recipient assigned by the recipient-MD, if the specified **recipient-name** does not identify an MTS-user. It may be generated by the originator of the message.

This argument may have one of the following values: **alternate-recipient-allowed** or **alternate-recipient-prohibited**.

If this argument has the value **alternate-recipient-allowed** and the **recipient-name** (specified by the originator of the message, or added by DL-expansion, or substituted by redirection to the **recipient-assigned-alternate-recipient** or to the **originator-requested-alternate-recipient**, or present by any combination of redirection and expansion) does not identify an MTS-user, the message may be redirected to an alternate-recipient assigned by the recipient-MD to receive such messages. If no such alternate-recipient has been assigned by the recipient-MD, or if this argument has the value **alternate-recipient-prohibited**, a non-delivery report shall be generated.

In the absence of this argument, the default **alternate-recipient-prohibited** shall be assumed.

Table 3 – Message-submission Arguments

Argument	Presence	Clause
<i>Originator Argument</i>		
Originator-name	M	8.2.1.1.1.1
<i>Recipient Arguments</i>		
Recipient-name	M	8.2.1.1.1.2
Alternate-recipient-allowed	O	8.2.1.1.1.3
Recipient-reassignment-prohibited	O	8.2.1.1.1.4
Originator-requested-alternate-recipient	O	8.2.1.1.1.5
DL-expansion-prohibited	O	8.2.1.1.1.6
Disclosure-of-other-recipients	O	8.2.1.1.1.7
DL-exempted-recipients	O	8.2.1.1.1.40
<i>Priority Argument</i>		
Priority	O	8.2.1.1.1.8
<i>Conversion Arguments</i>		
Implicit-conversion-prohibited	O	8.2.1.1.1.9
Conversion-with-loss-prohibited	O	8.2.1.1.1.10
Explicit-conversion	O	8.2.1.1.1.11

Table 3 – Message-submission Arguments

Argument	Presence	Clause
<i>Delivery Time Arguments</i>		
Deferred-delivery-time	O	8.2.1.1.1.12
Latest-delivery-time	O	8.2.1.1.1.13
<i>Delivery Method Argument</i>		
Requested-delivery-method	O	8.2.1.1.1.14
<i>Physical Delivery Arguments</i>		
Physical-forwarding-prohibited	O	8.2.1.1.1.15
Physical-forwarding-address-request	O	8.2.1.1.1.16
Physical-delivery-modes	O	8.2.1.1.1.17
Registered-mail-type	O	8.2.1.1.1.18
Recipient-number-for-advice	O	8.2.1.1.1.19
Physical-rendition-attributes	O	8.2.1.1.1.20
Originator-return-address	O	8.2.1.1.1.21
<i>Report Request Arguments</i>		
Originator-report-request	M	8.2.1.1.1.22
Content-return-request	O	8.2.1.1.1.23
Physical-delivery-report-request	O	8.2.1.1.1.24
<i>Security Arguments</i>		
Originator-certificate	O	8.2.1.1.1.25
Message-token	O	8.2.1.1.1.26
Content-confidentiality-algorithm-identifier	O	8.2.1.1.1.27
Content-integrity-check	O	8.2.1.1.1.28
Message-origin-authentication-check	O	8.2.1.1.1.29
Message-security-label	O	8.2.1.1.1.30
Proof-of-submission-request	O	8.2.1.1.1.31
Proof-of-delivery-request	O	8.2.1.1.1.32
Multiple-originator-certificates	O	8.2.1.1.1.41
Recipient-certificate	O	8.2.1.1.1.42
Certificate-selectors	O	8.2.1.1.1.43
Certificate-selectors-override	O	8.2.1.1.1.44
<i>Content Arguments</i>		
Original-encoded-information-types	O	8.2.1.1.1.33
Content-type	M	8.2.1.1.1.34
Content-identifier	O	8.2.1.1.1.35
Content-correlator	O	8.2.1.1.1.36
Content	M	8.2.1.1.1.37
Notification-type	O	8.2.1.1.1.38
Service-message	O	8.2.1.1.1.39

8.2.1.1.1.4 Recipient-reassignment-prohibited

This argument indicates whether the message may be reassigned to another MTS-user registered as a **recipient-assigned-alternate-recipient** by the intended-recipient. It may be generated by the originator of the message.

This argument may have one of the following values: **recipient-reassignment-prohibited** or **recipient-reassignment-allowed**.

If this argument has the value **recipient-reassignment-allowed** and the intended-recipient has registered an applicable **recipient-assigned-alternate-recipient**, the message shall be redirected to that **recipient-assigned-alternate-recipient**.

If this argument has the value **recipient-reassignment-prohibited** and the intended-recipient has registered an applicable **recipient-assigned-alternate-recipient**, then if an **originator-requested-alternate-recipient** has been specified by the originator of the message the message shall be redirected to the **originator-requested-alternate-recipient**, or if no **originator-requested-alternate-recipient** has been specified by the originator of the message, a non-delivery-report shall be generated.

In the absence of this argument, the default **recipient-reassignment-allowed** shall be assumed.

8.2.1.1.1.5 Originator-requested-alternate-recipient

This argument contains the **OR-name** of the alternate-recipient requested by the originator of the message. It may be generated by the originator of the message. A different value of this argument may be specified for each recipient of the message.

The **originator-requested-alternate-recipient** contains the **OR-name** of an individual, or DL, alternate-recipient.

If this argument is present and delivery of the message to the **recipient-name** (specified by the originator of the message, or added by DL-expansion, or substituted by redirection to a **recipient-assigned-alternate-recipient**) is not possible, the message shall be redirected to the **originator-requested-alternate-recipient** specified by this argument.

If an **originator-requested-alternate-recipient** has been specified by the originator of the message, the message shall be redirected to that alternate-recipient in preference to the one assigned by the recipient-MD.

8.2.1.1.1.6 DL-expansion-prohibited

This argument indicates whether DL-expansion within the MTS shall occur for any **recipient-name** which denotes a DL. It may be generated by the originator of the message.

This argument may have one of the following values: **DL-expansion-prohibited** or **DL-expansion-allowed**.

In the absence of this argument, the default **DL-expansion-allowed** shall be assumed.

8.2.1.1.1.7 Disclosure-of-other-recipients

This argument indicates whether the **recipient-name** of all recipients are to be indicated to each recipient MTS-user when the message is delivered. It may be generated by the originator of the message.

This argument may have one of the following values: **disclosure-of-other-recipients-requested** or **disclosure-of-other-recipients-prohibited**.

In the absence of this argument, the default **disclosure-of-other-recipients-prohibited** shall be assumed.

8.2.1.1.1.8 Priority

This argument specifies the relative priority of the message: **normal**, **non-urgent** or **urgent**. It may be generated by the originator of the message.

In the absence of this argument, a default **priority** of **normal** shall be assumed.

8.2.1.1.1.9 Implicit-conversion-prohibited

This argument indicates whether implicit-conversion may be performed on the message **content**. It may be generated by the originator of the message.

This argument may have one of the following values: **implicit-conversion-prohibited** or **implicit-conversion-allowed**.

In the absence of this argument, the default **implicit-conversion-allowed** shall be assumed.

See also 8.2.1.1.1.10.

8.2.1.1.1.10 Conversion-with-loss-prohibited

This argument indicates whether **encoded-information-type** conversion(s) may be carried out on the message **content**, if such conversion(s) would result in loss of information. Loss of information is defined in CCITT Rec. X.408. It may be generated by the originator of the message.

This argument may have one of the following values: **conversion-with-loss-prohibited** or **conversion-with-loss-allowed**.

In the absence of this argument, the default **conversion-with-loss-allowed** shall be assumed.

The combined effect of the **implicit-conversion-prohibited** and **conversion-with-loss-prohibited** arguments relate to implicit-conversion only and is defined in Table 4.

Table 4 – Combined Effect of Conversion Arguments

Implicit Conversion	Conversion With Loss	Combined Effect
allowed	with-loss-allowed	Allowed
allowed	with-loss-prohibited	with-loss-prohibited
prohibited	with-loss-allowed	prohibited
prohibited	with-loss-prohibited	prohibited

8.2.1.1.1.11 Explicit-conversion

This argument indicates the type of conversion of the message **content** explicitly requested by the originator for the recipient. It may be generated by the originator of the message. A different value of this argument may be specified for each recipient of the message.

This argument may have one of the following values: **ia5-text-to-teletex**, **ia5-text-to-g3-facsimile**, **ia5-text-to-g4-class-1**, **ia5-text-to-videotex**, **teletex-to-ia5-text**, **teletex-to-g3-facsimile**, **teletex-to-g4-class-1**, **teletex-to-videotex**, **videotex-to-ia5-text**, or **videotex-to-teletex**. Other types of **explicit-conversion** may be defined by addenda or future versions of this Recommendation | International Standard. **Explicit-conversion** shall be performed as specified in CCITT Rec. X.408.

In the absence of this argument, no explicit conversion shall be performed.

NOTE – When specified for a recipient DL, **explicit-conversion** applies to all members of the DL.

8.2.1.1.1.12 Deferred-delivery-time

This argument specifies the **Time** before which the message should not be delivered to the recipient(s). It may be generated by the originator of the message.

8.2.1.1.1.13 Latest-delivery-time

This argument contains the **Time** after which the message should not be delivered to the recipient(s). It may be generated by the originator of the message.

The handling of non-delivery because of expired **latest-delivery-time** is described in 14.3.2.4.

8.2.1.1.1.14 Requested-delivery-method

This argument indicates the preferred method of delivery of the message to the recipient. It may be generated by the originator of the message. A different value of this argument may be specified for each recipient of the message.

This argument may have one or more of the following values: **any-delivery-method**, **mhs-delivery**, **physical-delivery**, **telex-delivery**, **teletex-delivery**, **g3-facsimile-delivery**, **g4-facsimile-delivery**, **ia5-terminal-delivery**, **videotex-delivery**, or **telephone-delivery**.

If more than one value of this argument is specified for a recipient, the sequence of the values shall be assumed to imply the originator's order of preference of delivery-methods.

In the absence of this argument, the default **any-delivery-method** shall be assumed.

If the **recipient-name** generated by the originator of the message contains a **directory-name** but omits an **OR-address**, the MTS may use the **requested-delivery-method** as an indication of which form of **OR-address** the **directory-name** should be mapped to by the MTS (e.g., using the Directory). If an **OR-address** cannot be found, either a **recipient-improperly-specified** abstract-error or a non-delivery report shall be returned to the originator of the message.

If the originator-supplied **requested-delivery-method** conflicts with the recipient's preferred delivery-method (e.g., as registered in the Directory in the preferredDeliveryMethod attribute), the originator's **requested-delivery-method** takes precedence. If the originator's **requested-delivery-method** conflicts with the originator's conversion requirements (see clauses 8.2.1.1.1.9 to 8.2.1.1.1.11), a non-delivery report shall be returned to the originator of the message.

8.2.1.1.1.15 Physical-forwarding-prohibited

This argument indicates whether physical-forwarding of the message is prohibited. It may be generated by the originator of the message if the **requested-delivery-method** argument specifies that physical-delivery is required to the recipient, or if the originator of the message supplied a **postal-OR-address** for the recipient. A different value of this argument may be specified for each recipient of the message.

This argument may have one of the following values: **physical-forwarding-allowed**, or **physical-forwarding-prohibited**.

In the absence of this argument, the default **physical-forwarding-allowed** shall be assumed.

8.2.1.1.1.16 Physical-forwarding-address-request

This argument indicates whether the physical-forwarding-address of the recipient is to be returned in the report. It may be generated by the originator of the message if the **requested-delivery-method** argument specifies that physical-delivery is required to the recipient, or if the originator of the message supplied a **postal-OR-address** for the recipient. A different value of this argument may be specified for each recipient of the message.

This argument may have one of the following values: **physical-forwarding-address-requested** or **physical-forwarding-address-not-requested**.

In the absence of this argument, the default **physical-forwarding-address-not-requested** shall be assumed.

A physical-forwarding-address may be requested when physical-forwarding is prohibited or allowed (see 8.2.1.1.1.15).

8.2.1.1.1.17 Physical-delivery-modes

This argument indicates the mode of physical-delivery to the recipient to be used. It may be generated by the originator of the message if the **requested-delivery-method** argument specifies that physical-delivery is required to the recipient, or if the originator of the message supplied a **postal-OR-address** for the recipient. A different value of this argument may be specified for each recipient of the message.

This argument's value is the combination of two independent components. If present, the first component shall have one of the following values: **ordinary-mail**, **special-delivery**, **express-mail**, **counter-collection**, **counter-collection-with-telephone-advice**, **counter-collection-with-telex-advice**, or **counter-collection-with-teletex-advice**. If present, the second component shall have the value **bureau-fax-delivery**. When **bureau-fax-delivery** is requested and the first component is also present, then the first component is activated by the Bureau fax service.

Bureau-fax-delivery comprises all A to H modes of delivery defined in CCITT Rec. F.170, i.e.: A – Regular Delivery, B – Special Delivery, C – Express Mail, D – Counter Collection, E – Counter Collection with telephone advice, F – Telefax, G – Counter Collection with Telex advice, and H – Counter Collection with Teletex advice.

In the absence of this argument, the default **ordinary-mail** shall be assumed.

8.2.1.1.1.18 Registered-mail-type

This argument indicates the type of registered mail service to be used to physically deliver the message to the recipient. It may be generated by the originator of the message if the **requested-delivery-method** argument specifies that physical-delivery is required to the recipient, or if the originator of the message supplied a **postal-OR-address** for the recipient. A different value of this argument may be specified for each recipient of the message.

This argument may have one of the following values: **non-registered-mail**, **registered-mail**, or **registered-mail-to-addressee-in-person**.

In the absence of this argument, the default **non-registered-mail** shall be assumed.

8.2.1.1.1.19 Recipient-number-for-advice

This argument contains the Telephone, Telex or Teletex number of the recipient, to be used in conjunction with the **counter-collection-with-advice** and **bureau-fax-delivery physical-delivery-modes**. It may be generated by the originator of the message if the **requested-delivery-method** argument specifies that physical-delivery is required to the recipient, or if the originator of the message supplied a **postal-OR-address** for the recipient, and the **physical-delivery-modes** argument specifies a **counter-collection-with-advice** or **bureau-fax-delivery physical-delivery-mode**. A different value of this argument may be specified for each recipient of the message.

8.2.1.1.1.20 Physical-rendition-attributes

This argument indicates the **physical-rendition-attributes** to be applied when the message is rendered into physical form. It may be generated by the originator of the message if the message is likely to require rendition, for example if the recipient address designates an access unit, or if the **requested-delivery-method** specifies a delivery method involving an access unit. A different value of this argument may be specified for each recipient of the message.

This argument is specified as an Object Identifier. The following values are defined in this specification:

basic No special rendition is required – the normal rendition offered by the AU should be applied.

no-cover-page The message should be rendered without the addition of any cover page supplied by the AU. This value is particularly appropriate for facimile access units.

Other values of this argument may be registered privately and used by agreement. Addenda or future versions of this Recommendation | International Standard may define other standardised values.

In the absence of this argument, the default **basic** shall be assumed.

8.2.1.1.1.21 Originator-return-address

This argument contains the **postal-OR-address** of the originator of the message. It may be generated by the originator of the message if the **requested-delivery-method** argument specifies that physical-delivery is required to one or more recipients of the message, or if the originator of the message supplied one or more **postal-OR-addresses** for the recipients. It may also be generated by the originator of the message if a recipient DL contains, or is likely to contain, one or more members for whom physical-delivery is required.

The **originator-return-address** shall contain the **postal-OR-address** of an individual originator (**OR-address**), i.e., shall not contain the **directory-name** of an individual originator nor the **directory-name** of a DL.

8.2.1.1.1.22 Originator-report-request

This argument indicates the kind of report requested by the originator of the message. It shall be generated by the originator of the message. A different value of this argument may be specified for each recipient of the message.

This argument may have one of the following values:

no-report: the originator of the message requested the suppression of non-delivery-reports;

non-delivery-report: a report is returned only in case of non-delivery;

report: a report is returned in case of delivery or non-delivery.

The value of this argument may be changed at a DL expansion-point in line with the reporting-policy of the DL. Such a change may affect the number and type of reports the originator of the message may receive about delivery to a DL.

8.2.1.1.1.23 Content-return-request

This argument indicates whether the message **content** is to be returned with any non-delivery-report(s). It may be generated by the originator of the message.

This argument may have one of the following values: **content-return-requested** or **content-return-not-requested**.

In the absence of this argument, the default **content-return-not-requested** shall be assumed.

The suppression of non-delivery-reports by the originator of the message (see 8.2.1.1.1.22) takes precedence over a request for the return of the **content**.

In the case of non-delivery-reports delivered to the owner of a DL (see 8.3.1.2.1.4), the message **content** shall not be present.

8.2.1.1.1.24 Physical-delivery-report-request

This argument indicates the type of physical-delivery-report requested by the originator of the message. It may be generated by the originator of the message if the **requested-delivery-method** argument specifies that physical-delivery is required to the recipient or if the originator of the message supplied a **postal-OR-address** for the recipient. A different value of this argument may be specified for each recipient of the message.

This argument may have one of the following values: **return-of-undeliverable-mail-by-PDS**, **return-of-notification-by-PDS**, **return-of-notification-by-MHS**, or **return-of-notification-by-MHS-and-PDS**.

In the absence of this argument, the default **return-of-undeliverable-mail-by-PDS** shall be assumed.

8.2.1.1.1.25 Originator-certificate

This argument contains a **certificate** of the originator of the message. It shall be generated by a trusted source (e.g., a certification-authority), and may be supplied by the originator of the message.

The **originator-certificate** may be used to convey a verified copy of the public-asymmetric-encryption-key (**subject-public-key**) of the originator of the message.

NOTE – If more than one originator certificate is required to be conveyed to all recipients, then the certificate for **message-origin-authentication-check** is conveyed in this argument and the other certificates are conveyed in the **multiple-originator-certificates** argument. If dedicated certificates are required for each recipient, then the dedicated certificates are identified in the **certificates-selectors-override** argument (see 8.2.1.1.1.44).

When the same algorithm and secret key has been used to compute digital signatures conveyed in one or more of the following arguments, **message-origin-authentication-check**, **content-integrity-check** or **message-token** argument, then the corresponding originator's public-asymmetric-encryption-key may be used by the recipients of the message to validate digital signatures conveyed in the **content-integrity-check** argument and the **message-token** argument if an **asymmetric-token** is used with an asymmetric algorithm (see 8.5.8). It may also be used by the recipients of the message, and any MTA through which the message is transferred, to validate the **message-origin-authentication-check**.

8.2.1.1.1.26 Message-token

This argument contains the **token** associated with the message. It may be generated by the originator of the message. A different value of this argument may be specified for each recipient of the message.

If the **message-token** is an **asymmetric-token**, the **signed-data** may comprise:

any of the following arguments: the **content-confidentiality-algorithm-identifier**, the **content-integrity-check**, the **message-security-label**, and the **proof-of-delivery-request**; and

a **message-sequence-number**, that identifies the position of the message in a sequence of messages from the originator to the recipient to which the **message-token** relates (to provide the Message Sequence Integrity element-of-service, as defined in ITU-T Rec. X.400 | ISO/IEC 10021-1). The first occurrence of a sequence number can be a random number.

If the **message-token** is an **asymmetric-token**, the **encrypted-data** may comprise:

a **content-confidentiality-key**: a symmetric-encryption-key used with the **content-confidentiality-algorithm-identifier** by the originator of the message to encrypt the message content, and by the recipient to decrypt the message **content**; and/or

the **content-integrity-check**: may be included in the **encrypted-data** if confidentiality of the **content-integrity-check** is required, and/or if the **message-security-label** is included in the **encrypted-data** (for confidentiality of the message-security-label) and the association between the content-integrity-check and the message-security-label is to be maintained;

the **message-security-label**: may be included in the **encrypted-data** if confidentiality of the **message-security-label** is required;

a **content-integrity-key**: a symmetric-encryption-key used with the **content-integrity-algorithm-identifier** by the originator of the message to compute the **content-integrity-check**, and by the recipient to validate the **content-integrity-check**;

a **message-sequence-number**: as defined for the **signed-data** above, but may be included in the **encrypted-data** if confidentiality of the sequence is required. The first occurrence of a sequence number can be a random number.

If the **message-token** is an **asymmetric-token** and the **signed-data** of the **message-token** includes the **content-integrity-check**, the **message-token** may provide non-repudiation-of-origin of the message **content** subject to availability of an appropriate Public Key infrastructure (the Non Repudiation of Origin element-of-service, as defined in ITU-T Rec. X.400 | ISO/IEC 10021-1). If the **signed-data** of the **message-token** includes both the **content-integrity-check** and the **message-security-label**, the **message-token** provides proof of association between the **message-security-label** and the message **content**.

Symmetric algorithms may be used within the above **asymmetric-token** (see 8.5.8). If symmetric algorithms are used for both the **message-token** and the **content-integrity-check** then the **message-token** can only support Non Repudiation of Origin elements-of-service if the security policy in force provides for the involvement of a third party acting as a notary.

NOTE 1 – If multiple certificates are required to be exchanged to process the **message-token**, then certificates may be conveyed in the **multiple-originator-certificates** argument, the **recipient-certificate** argument, or both.

NOTE 2 – A certificate needed to implement a key agreement for the encrypted-data of the token may use an originator certificate in the **multiple-originator-certificates** argument, together with the recipient certificate in the **recipient-certificate** argument. The appropriate certificate may be identified using Version 3 certificates, which contains certificate extensions for this purpose; the identification may be conveyed in the **certificate-selectors** and **certificate-selectors-override** arguments. (For example, the **key usage** field may be used to indicate the certificate is to be used for key agreement purposes and **certificate policies** field may be used to indicate the policy under which the key agreement is to operate.)

8.2.1.1.1.27 Content-confidentiality-algorithm-identifier

This argument contains an **algorithm-identifier**, which identifies the algorithm used by the originator of the message to encrypt the message **content** (to provide the Content Confidentiality element-of-service as defined in ITU-T Rec. X.400 | ISO/IEC 10021-1). It may be generated by the originator of the message.

The algorithm may be used by the recipient(s) of the message to decrypt the message **content**.

The content-confidentiality algorithm may be either a symmetric- or an asymmetric-encryption-algorithm.

If a symmetric-encryption-algorithm is used, the **content-confidentiality-key** used by the originator to encrypt the message **content**, and which the recipient may use to decrypt the message **content**, may be derived from the **message-token** sent with the message. Alternatively, the **content-confidentiality-key** may be distributed by some other means.

If an asymmetric-encryption-algorithm is used, the intended-recipient's public-asymmetric-encryption-key may be used by the originator of the message to encrypt the message **content**. The recipient may use the recipient's secret-asymmetric-encryption-key to decrypt the message **content**. If an asymmetric-encryption-algorithm is used, the message can only be addressed to a single recipient, or to a set of recipients which share the same asymmetric-encryption-key pair.

8.2.1.1.1.28 Content-integrity-check

This argument provides the recipient of the message with a means of validating that the message **content** has not been modified (to provide the Content Integrity element-of-service as defined in ITU-T Rec. X.400 | ISO/IEC 10021-1). It may be generated by the originator of the message. A different value of the argument may be specified for each recipient of the message.

If the value of this argument is specific to a recipient, because either a specific algorithm or key has been used to generate this value (i.e. when different values of the argument are specified for each recipient of the message), then the appropriate certificates may be conveyed by the **multiple-originator-certificates** argument and identified by the **certificate-selectors-override** argument.

If the same algorithm and key has been used to generate this argument for all recipients (i.e. the same value of the argument is specified for each recipient of the message), then the appropriate certificate may be conveyed by the **originator-certificate** argument, or if more than one originator's certificate is to be conveyed the **multiple-originator-certificates** argument shall be used and the appropriate certificate identified by the **certificate-selectors** and **certificate-selectors-override** arguments.

This argument allows the recipient of the message to validate the integrity of the message content received and the authentication of the originator of the message.

The **content-integrity-check** enables content-integrity to be validated on a per-recipient basis using either a symmetric- or an asymmetric-encryption-algorithm.

NOTE 1 – The **message-origin-authentication-check** provides a means of validating content-integrity on a per-message basis using an asymmetric-encryption-algorithm.

The **content-integrity-check** may also be included in the **signed-data** or the **encrypted-data** of the **message-token** to provide for non-repudiation-of-origin of the message **content** subject to availability of an appropriate Public Key infrastructure, and proof of association between the **message-security-label** and the message **content**.

NOTE 2 – Thus, there are three separate arguments of **content-integrity-check**, one per recipient argument and two in the **message-token**.

The **content-integrity-check** is computed using the algorithm identified by the **content-integrity-algorithm-identifier** (an **algorithm-identifier**).

NOTE 3 – The various **CONTENT-INTEGRITY-CHECK** arguments may be computed using different algorithms. In particular, when the **CONTENT-INTEGRITY-CHECK** is included in the **SIGNED-DATA** or the **ENCRYPTED-DATA** of the **MESSAGE-TOKEN**, it may be computed using a different algorithm from the per recipient **content-integrity-check** argument.

The **content-integrity-check** contains the **content-integrity-algorithm-identifier**, and a digital signature which is generated using one or more encrypted functions (e.g., compressed, single hash, or double hashed version) over the message **content**, and conditionally over the **content-integrity-algorithm-identifier**.

NOTE 4 – The **content-integrity-check** could be computed using the clear (i.e., unencrypted) or the encrypted content. This choice can be made independently for each occurrence of the content integrity check in the message. This choice is dictated by the security policy in force and may also be indicated by **content-integrity-algorithm-identifier**.

The **content-integrity-algorithm-identifier** shall specify:

- 1) whether the **content-integrity-check** is computed using the clear (i.e. unencrypted) or the encrypted **content**, if this is not dictated by the security policy;
- 2) the presence or absence of the **content-integrity-algorithm-identifier** within the ASN.1 sequence on which the signature is computed;
- 3) the ASN.1 encoding rule (CER or DER) to be applied to the ASN.1 sequence before hashing;
- 4) the hash function;

- 5) whether or not the hash value is to be encoded within an ASN.1 Bit String prior to encryption;
- 6) the algorithm used to protect the hash value (e.g. an asymmetric encryption algorithm); and
- 7) any parameters of the algorithm such as any necessary keys, initialization values, and padding instructions.

The content-integrity algorithm may be either a symmetric- or an asymmetric-encryption-algorithm.

If a symmetric-encryption-algorithm is used, the **content-integrity-key** used to compute the **content-integrity-check**, and which the recipient may use to validate the **content-integrity-check**, may be derived from the **message-token** sent with the message. Alternatively, the **content-integrity-key** may be distributed by some other means.

NOTE 5 – The use of a symmetric-encryption-algorithm may permit simultaneous compression and encryption of the message **content** to create the **content-integrity-check**.

If an asymmetric-encryption-algorithm is used, the originator's secret-asymmetric-encryption-key may be used by the originator of the message to compute the **content-integrity-check**. The recipient may use the originator's public-asymmetric-encryption-key (**subject-public-key**) derived from the **originator-certificate** or **multiple-originator-certificates** to validate the appropriate **content-integrity-check** value.

NOTE 6 – When multiple certificates are required, the appropriate certificate can be identified from the **certificate-selectors** and **certificate-selectors-override** arguments by use of the **key usage** extension or **certificate policies** extension defined in ITU-T Rec. X.509 | ISO/IEC 9594-8, or by a combination of both. For example, the certificate required to validate a per recipient digital signature (the value of a per recipient **content-integrity-check**) may be identified by the **certificate-selectors-override** delivered to the recipient: if more than one certificate is delivered to this user, the appropriate certificate can be determined by **key usage** and **certificate policies** extension (i.e. **key usage** will be **digitalSignature**, the object identifier in the **certificate policies** extension may indicate the policy under which the signature was generated and is to be used, and this policy in turn may define in what domains the signature is valid).

8.2.1.1.1.29 Message-origin-authentication-check

This argument provides the recipient(s) of the message, and any MTA through which the message is transferred, with a means of authenticating the origin of the message (to provide the Message Origin Authentication element-of-service as defined in ITU-T Rec. X.400 | ISO/IEC 10021-1). It may be generated by the originator of the message.

The **message-origin-authentication-check** provides proof of the origin of the message (Message Origin Authentication), assurance that the message **content** has not been modified (the Content Integrity element-of-service as defined in ITU-T Rec. X.400 | ISO/IEC 10021-1), and proof of association between the **message-security-label** and the message.

The **message-origin-authentication-check** is computed using the algorithm (asymmetric-encryption-algorithm and hash-function) identified by the **message-origin-authentication-algorithm-identifier** (an **algorithm-identifier**).

The **message-origin-authentication-check** contains the **message-origin-authentication-algorithm-identifier**, and an asymmetrically-encrypted hashed version of: the **message-origin-authentication-algorithm-identifier**; the message **content**; the **content-identifier** and the **message-security-label**. Optional components are included in the **message-origin-authentication-check** if they are present in the message.

If content-confidentiality (see 8.2.1.1.1.27) is also used, the **message-origin-authentication-check** is computed using the encrypted version of the message **content** (to allow the **message-origin-authentication-check** to be validated by other than the intended-recipient (e.g., by an MTA) without compromising the confidentiality of the message **content**). If the clear (i.e., unencrypted) version of the message **content** is used to compute the **message-origin-authentication-check**, the **message-origin-authentication-check** provides for both Message Origin Authentication and Non Repudiation of Origin of the message **content** (a signature), as defined in ITU-T Rec. X.400 | ISO/IEC 10021-1. If, however, the encrypted version of the message **content** is used, the **message-origin-authentication-check** provides for Message Origin Authentication, but not for Non Repudiation of Origin of the message **content**.

The **message-origin-authentication-check** may be computed by the originator of the message using the originator's secret-asymmetric-encryption-key. The **message-origin-authentication-check** may be validated by the recipient(s) of the message, and any MTA through which the message is transferred, using the public-asymmetric-encryption-key (**subject-public-key**) of the originator of the message derived from the **originator-certificate**.

Addenda or future versions of this Recommendation | International Standard may define other forms of **message-origin-authentication-check** (e.g., based on symmetric-encryption-techniques) which may be used by MTAs through which the message is transferred to authenticate the origin of the message.

8.2.1.1.1.30 Message-security-label

This argument associates a **security-label** with the message (or probe). It may be generated by the originator of the message (or probe), in line with the security-policy in force.

The **message-security-label** of a report shall be the same as the **message-security-label** of the subject-message (or -probe).

If **security-labels** are assigned to MTS-users, MTAs and other objects in the MHS, the handling, by those objects, of messages, probes and reports bearing **message-security-labels** may be determined by the security-policy in force. If security-labels are not assigned to MTS-users, MTAs and other objects in the MHS, the handling, by those objects, of messages, probes and reports bearing **message-security-labels** may be discretionary.

If security-contexts are established between the originator and an MTA (the originating-MTA) of the MTS (see clauses 8.1.1.1.1.3 and 8.2.1.4.1.5), the **message-security-label** that the originator may assign to a message (or probe) may be determined by the **security-context** (submission-security-context), in line with the security-policy in force. If **security-contexts** are not established between the originator and the originating-MTA, the assignment of a **message-security-label** to a message (or probe) may be at the discretion of the originator.

If **security-contexts** are established between two MTAs (see 12.1.1.1.1.3), the transfer of messages, probes or reports between the MTAs may be determined by the **message-security-labels** of the messages, probes or reports, and the **security-context**, in line with the security-policy in force. If **security-contexts** are not established between the MTAs, the transfer of messages, probes and reports may be at the discretion of the sender.

If **security-contexts** are established between an MTS-user and an MTA (the delivering-MTA) of the MTS (see clauses 8.1.1.1.1.3 and 8.3.1.3.1.7), the delivery of messages and reports may be determined by the **message-security-labels** of the messages and reports, and the **security-context** (delivery-security-context), in line with the security-policy in force. If the **message-security-label** of a message or report is allowed by the registered **user-security-labels** of the recipient, but disallowed by the recipient's current **security-context** (delivery-security-context), then the delivering-MTA may hold-for-delivery. If **security-contexts** are not established between the MTS-user and the delivering-MTA, the delivery of messages and reports may be at the discretion of the delivering-MTA.

8.2.1.1.1.31 Proof-of-submission-request

This argument indicates whether or not the originator of the message requires **proof-of-submission** (to provide the Proof of Submission element-of-service) as defined in ITU-T Rec. X.400 | ISO/IEC 10021-1) of the message to the MTS. It may be generated by the originator of the message.

This argument may have one of the following values: **proof-of-submission-requested** or **proof-of-submission-not-requested**.

In the absence of this argument, the default **proof-of-submission-not-requested** shall be assumed.

8.2.1.1.1.32 Proof-of-delivery-request

This argument indicates whether or not the originator of the message requires **proof-of-delivery** (to provide the Proof of Delivery element-of-service as defined in ITU-T Rec. X.400 | ISO/IEC 10021-1) of the message to the recipient. It may be generated by the originator of the message. A different value of this argument may be specified for each recipient of the message.

This argument may have one of the following values: **proof-of-delivery-requested** or **proof-of-delivery-not-requested**.

In the absence of this argument, the default **proof-of-delivery-not-requested** shall be assumed.

8.2.1.1.1.33 Original-encoded-information-types

This argument identifies the original **encoded-information-types** of the message **content**. It may be generated by the originator of the message.

The absence of this argument indicates that the **original-encoded-information-types** of the message **content** are **unspecified**.

8.2.1.1.1.34 Content-type

This argument identifies the type of the **content** of the message. It identifies the abstract syntax and the encoding rules used. It shall be generated by the originator of the message. The **content-type** shall be either built-in or extended.

A built-in **content-type** may have one of the following values:

unidentified: denotes a **content-type** unidentified and unconstrained; the use of this is by bilateral agreement between MTS-users;

external: denotes a **content-type** which is reserved for use when interworking between 1988 systems and 1984 systems; it shall only be used with **mts-transfer-protocol-1984** (see ITU-T Rec. X.419 | ISO/IEC 10021-6);

NOTE – The interworking rules ensure that the **external content-type** is never used in conjunction with **mts-transfer** or **mts-transfer-protocol**. Although the **external content-type** is designed to allow interworking between 1988 systems through intermediate 1984 systems, a 1984 system may deliver (or submit) a **content** of the **external content-type** provided that the MTS-user (or the MTA itself) performs the equivalent of the upgrading (or downgrading) rules given in ITU-T Rec. X.419 | ISO/IEC 10021-6.

interpersonal-messaging-1984: identifies the defined in ITU-T Rec. X.420 | ISO/IEC 10021-7;

interpersonal-messaging-1988: identifies the defined in ITU-T Rec. X.420 | ISO/IEC 10021-7;

edi-messaging: identifies the **edim content-type** defined in ITU-T Rec. X.435 | ISO/IEC 10021-9;

voice-messaging: identifies the **vm content-type** defined in ITU-T Rec. X.440.

An extended **content-type** is specified using an object identifier.

One specific value of an extended **content-type** which has been defined by this Service Definition is:

inner-envelope: an extended **content-type** that is itself a message (envelope and content). When delivered to the recipient named on the outer-envelope, the outer-envelope is removed and the content is deciphered, if needed, resulting in an inner-envelope and its content. The information contained in the inner-envelope is used to transfer the content of the inner-envelope to the recipients named on the inner-envelope. The type of the **content** OCTET STRING is an **MTS-APDU** (see Figure 6 in ITU-T Rec. X.419 | ISO/IEC 10021-6) encoded using the Basic Encoding Rules of ASN.1. (The inner-envelope and content may be protected by securing the **content** of the outer-envelope using the security arguments (see clauses 8.2.1.1.1.25 to 8.2.1.1.1.32).)

Other standardised extended **content-types** may be defined by other MHS Specifications or other Recommendations | International Standards. Other values of this argument may be used by bilateral agreement between MTS-users.

NOTE – In the case where the content confidentiality service is used, the syntax and encoding identified by the **content-type** are the syntax and encoding of the content before encryption.

8.2.1.1.1.35 Content-identifier

This argument contains an identifier for the **content** of the message. It may be generated by the originator of the message.

The **content-identifier** may be delivered to the recipient(s) of the message, and is returned to the originator with any report(s). This argument is not altered by the MTS.

8.2.1.1.1.36 Content-correlator

This argument contains information to enable correlation of the **content** of the message by the originator of the message. It may be generated by the originator of the message.

The **content-correlator** is not delivered to the recipient(s) of the message, but is returned to the originator with any report(s). This argument is not altered by the MTS.

8.2.1.1.1.37 Content

This argument contains the information the message is intended to convey to the recipient(s). It shall be generated by the originator of the message.

Except when conversion is performed, the **content** of the message is not modified by the MTS, but rather is passed transparently through it.

The **content** may be encrypted to ensure its confidentiality (see 8.2.1.1.1.27).

NOTE – The value of the octet string containing the **encoded** content does not change as the message crosses the MTS.

8.2.1.1.1.38 Notification-type

This argument indicates that the **content** is a notification, and indicates that it is one of three types of notification (type-1, type-2 or type-3); the use of these values is defined in the relevant **content** specification. It may be generated by the originator of the message, but shall be generated only if the **content** is a notification as defined in the relevant **content** specification.

The **notification-type** indication is not delivered to the recipient(s) of the message and is not returned to the originator with any report(s). Depending upon policy, this argument may be verified by the MTS.

8.2.1.1.1.39 Service-message

This argument indicates that the message is for service purposes. It may be generated by the originator of the message, but shall be used only by bilateral agreement.

The **service-message** indication is not delivered to the recipient(s) of the message and is not returned to the originator with any report(s). Depending upon policy, this argument may be verified by the MTS.

8.2.1.1.1.40 DL-exempted-recipients

This argument contains the **OR-names** of potential recipients that are requested not to be added to the set of intended recipients as a result of DL-expansion. It may be generated by the originator of the message.

This argument remains unchanged during MTA processing and is included in subsequent transfer operations regardless of whether DL-expansion has already taken place.

The **DL-exempted-recipients** argument is delivered to the recipient(s), but is not returned to the originator with any report(s).

8.2.1.1.1.41 Multiple-originator-certificates

This argument contains a **certificate** of the originator of the message, or the **directory-name** of an entry in the Directory which contains a certificate of the originator, or multiple certificates (or directory-names) where the certificates contain different certification paths or are issued by different certification authorities or have different purposes. Each **certificate** shall be generated by a trusted source (e.g. a certification-authority), and may be supplied by the originator of the message.

The **multiple-originator-certificates** may be used to convey verified copies of public information of the originator needed to verify digital signatures or to be used for key agreement purposes. It may convey the public-asymmetric-encryption-key (**subject-public-key**) of the originator of the message, or other public information needed for key agreement processing.

Multiple **certificates** or **directory-names** may occur where more than one type of verified information of the originator of the message is to be conveyed.

NOTE 1 – If dedicated certificates are required for each recipient, then these dedicated certificates are identified in the **certificate-selectors-override** argument.

NOTE 2 – To implement a key agreement it may be necessary to have certificates in both the **multiple-originator-certificates** and the **recipient-certificate** arguments.

When a certificate within a **multiple-originator-certificates** is to be used for a particular purpose, Version 3 certificates (see ITU-T Rec. X.509 | ISO/IEC 9594-8) shall be used to indicate the purpose of the information contained in the certificate. The **key usage** and **certificate policies** extension of Version 3 certificates may be used individually, or in combination, to indicate the purpose of a certificate conveyed in the **multiple-originator-certificates** element. The **key usage** and **certificate policies** extension may indicate when the originator's public-asymmetric-encryption-key is needed to validate a digital signature in any one of the following arguments, **message-origin-authentication-check**, **content-integrity-check** or **message-token**. Also, if more than one value of digital signature is conveyed using the various content-integrity-check arguments, the appropriate certificate may be indicated by the combination of the **key usage** and **certificate policies** certificate extensions. The **key usage** and **certificate policies** extension may indicate when the originator's public information is needed for key agreement proposes in processing the **message-token** argument.

Several digital signatures may be generated by the originator of a message, which are conveyed in the **message-origin-authentication-check**, **content-integrity-check** and/or **message-token** arguments. If the same algorithm and originator's public-asymmetric-key is needed to validate all the digital signatures, this may be indicated by the combination of the **key usage** and **certificate policies** certificate extensions.

NOTE 3 – If dedicated algorithms and originator's public-asymmetric-keys are needed to verify digital signatures for each recipient, then dedicated certificates are also required for each recipient. In this case, the dedicated certificate is identified in the **certificate-selectors-override** argument.

8.2.1.1.1.42 Recipient-certificate

This argument contains a **certificate** of the recipient of the message and optionally its certification path. The **certificate** shall be generated by a trusted source (e.g. a certification-authority), and may be supplied by the originator of the message. A different value of this argument may be specified for each recipient of the message.

The **recipient-certificate** may be used to convey a verified copy of public information to be used for key agreement purposes. It identifies the public-asymmetric-encryption-key (**subject-public-key**) of the recipient of the message which was used by the originator. This identification may alternatively be conveyed in the **certificate-selectors-override** argument. Such identification is necessary only if the recipient has more than one certificate for the identified algorithm.

The certificate conveyed in the **recipient-certificate** may be used for key agreement purposes, such as generating keys needed to process the **encrypted-data** in the **message-token**.

If the message is expanded by one or more secure DLs in the message path, the **recipient-certificate** may be generated by the DL.

8.2.1.1.1.43 Certificate-selectors

This argument contains information sufficient to identify one **certificate** where a user has more than one **certificate** with the same **algorithm-identifier**. It allows a **certificate** of the originator to be identified to validate specific digital signatures within the **message-origin-authentication-check**, **content-integrity-check**, or **message-token** arguments, or to be used for key agreement for encryption. It also allows a certificate of each recipient to be identified for key agreement or asymmetric encryption. It may be generated by the originator of the message.

Each component of **certificate-selectors** allows any certificate selection criteria specified for Certificate Match in 12.7.2 of ITU-T Rec. X.509 | ISO/IEC 9594-8 which is applicable to a user certificate. The recipient adds the appropriate algorithm-identifier (into **subjectPublicKeyAlgID**) and the message submission (or token creation) time on which the certificate and private key were valid (into **certificateValid** and **privateKeyValid**) to the originator's specified selection criteria before selecting a certificate. The specified criteria when combined together with these values shall be sufficient to select one certificate. For example, this allows unique identification of a single certificate by **issuer** and **serial-number**, or generic identification of a class of certificate by **key-purpose** or **certificate-policy** (which, when combined with the appropriate algorithm-identifier and validity date, will yield a single certificate for each user). The value in each component applies to all recipients unless there is a value in the corresponding component of **certificate-selectors-override** for that recipient. The identified certificates may (but need not) be present in the **originator-certificate** or **multiple-originator-certificates** arguments.

The **certificate-selectors** argument contains the following components:

encryption-recipient
encryption-originator
content-integrity-check
token-signature
message-origin-authentication

The *encryption-recipient* identifies one of the recipient's certificates; each of the others identifies one of the originator's certificates. The first two apply to token-encryption if content-confidentiality-algorithm is symmetric, and to content-encryption if it is asymmetric.

8.2.1.1.1.44 Certificate-selectors-override

This argument contains information sufficient to identify one **certificate** where a user has more than one **certificate** with the same **algorithm-identifier**. It allows a **certificate** of the originator to be identified to validate specific digital signatures within the **content-integrity-check** or **message-token** arguments, or to be used for key agreement for encryption. It also allows a certificate of each recipient to be identified for key agreement or asymmetric encryption. It may be generated by the originator of the message. A different value of this argument may be specified for each recipient of the message.

This argument is identical to the **certificate-selectors** argument, except that it does not contain the *message-origin-authentication* component.

If this argument is present, then the value in each component that is present replaces the value in the corresponding component of the **certificate-selectors** argument for this recipient.

8.2.1.1.2 Results

Table 5 lists the results of the Message-submission abstract-operation, and for each result qualifies its presence and identifies the clause in which the result is defined.

Table 5 – Message-submission Results

Result	Presence	Clause
Message-submission-identifier	M	8.2.1.1.2.1
Message-submission-time	M	8.2.1.1.2.2
Originating-MTA-certificate	O	8.2.1.1.2.3
Proof-of-submission	C	8.2.1.1.2.4
Content-identifier	C	8.2.1.1.1.35

8.2.1.1.2.1 Message-submission-identifier

This result contains an **MTS-identifier** that uniquely and unambiguously identifies the message-submission. It shall be generated by the MTS.

The MTS provides the **message-submission-identifier** when notifying the MTS-user, via the Report-delivery abstract-operation, of the delivery or non-delivery of the message.

The MTS-user provides the **message-submission-identifier** when cancelling, via the Cancel-deferred-delivery abstract-operation, a message whose delivery it deferred.

8.2.1.1.2.2 Message-submission-time

This result indicates the **Time** at which the MTS accepts responsibility for the message. It shall be generated by the MTS.

8.2.1.1.2.3 Originating-MTA-certificate

This result contains the **certificate** of the MTA to which the message has been submitted (the originating-MTA). It shall be generated by a trusted source (e.g., a certification-authority), and may be supplied by the originating-MTA, if the originator of the message requested **proof-of-submission** (see 8.2.1.1.1.31) and an asymmetric-encryption-algorithm is used to compute the **proof-of-submission**.

The **originating-MTA-certificate** may be used to convey to the originator of the message a verified copy of the public-asymmetric-encryption-key (**subject-public-key**) of the originating-MTA.

The originating-MTA's public-asymmetric-encryption-key may be used by the originator of the message to validate the **proof-of-submission**.

8.2.1.1.2.4 Proof-of-submission

This result provides the originator of the message with proof of submission of the message to the MTS (to provide the Proof of Submission element-of-service as defined in ITU-T Rec. X.400 | ISO/IEC 10021-1). Depending on the encryption-algorithm used and the security policy in force, this argument may also provide the Non Repudiation of Submission element-of-service (as defined in ITU-T Rec. X.400 | ISO/IEC 10021-1). It shall be generated by the originating-MTA of the MTS, if the originator of the message requested **proof-of-submission** (see 8.2.1.1.1.31).

The **proof-of-submission** is computed using the algorithm identified by the **proof-of-submission-algorithm-identifier** (an **algorithm-identifier**).

The **proof-of-submission** contains the **proof-of-submission-algorithm-identifier**, and an encrypted function (e.g., a compressed or hashed version) of the **proof-of-submission-algorithm-identifier**, the Message-submission arguments (see 8.2.1.1.1) of the subject message, and the **message-submission-identifier** and **message-submission-time**.

Receipt of this result provides the originator of the message with Proof of Submission of the message. Non-receipt of this result provides neither Proof of Submission nor proof of non-submission (unless a secure link and trusted functionality are employed).

If an asymmetric-encryption-algorithm is used, the **proof-of-submission** may be computed by the originating-MTA using the originating-MTA's secret-asymmetric-encryption-key. The originator of the message may validate the **proof-of-submission** using the originating-MTA's public-asymmetric-encryption-key (**subject-public-key**) derived from the **originating-MTA-certificate**. An asymmetric **proof-of-submission** may also provide for Non Repudiation of Submission subject to availability of an appropriate Public Key infrastructure.

If a symmetric-encryption-algorithm is used, the symmetric-encryption-key that the originating-MTA used to compute the **proof-of-submission**, and which the originator may use to validate the **proof-of-submission**, may be derived from the **bind-tokens** (see clauses 8.1.1.1.1.3 and 8.1.1.1.2.2) exchanged when the association was initiated. Alternatively, the symmetric-encryption-key used for **proof-of-submission** may be exchanged by some other means. If a symmetric-encryption-algorithm is used then the **proof-of-submission** can only support Non Repudiation of Submission if the security-policy in force provides for the involvement of a third party acting as a notary.

8.2.1.1.3 Abstract-errors

Table 6 lists the abstract-errors that may disrupt the Message-submission abstract-operation, and for each abstract-error identifies the clause in which the abstract-error is defined.

Table 6 – Message-submission Abstract-errors

Abstract-error	Clause
Submission-control-violated	8.2.2.1
Element-of-service-not-subscribed	8.2.2.2
Originator-invalid	8.2.2.4
Recipient-improperly-specified	8.2.2.5
Inconsistent-request	8.2.2.7
Security-error	8.2.2.8
Unsupported-critical-function	8.2.2.9
Remote-bind-error	8.2.2.10

8.2.1.2 Probe-submission

The Probe-submission abstract-operation enables an MTS-user to submit a probe in order to determine whether or not a message (the subject-message) could be transferred and delivered to one or more recipient MTS-users if it were to be submitted.

Success of a probe does not guarantee that a subsequently submitted message can actually be delivered, but rather that, currently, the recipient is valid and the message would encounter no major obstacles to delivery.

For any **recipient-names** that denote a DL, the Probe-submission abstract-operation determines whether expansion of the specified DL (but not of any nested DLs) would occur.

For any **recipient-names** for which redirection would occur, the Probe-submission abstract-operation determines whether the message could be transferred and delivered to the replacement recipient.

The MTS-user supplies most of the arguments used for message-submission and the length of the content of the subject-message. The Probe-submission abstract-operation does not culminate in delivery to the intended recipients of the subject-message, but establishes whether or not the Message-submission abstract-operation would be likely to do so.

The successful completion of the abstract-operation signifies that the MTS has agreed to undertake the probe (but not that it has yet performed the probe).

The disruption of the abstract-operation by an abstract-error indicates that the MTS cannot undertake the probe.

8.2.1.2.1 Arguments

Table 7 lists the arguments of the Probe-submission abstract-operation, and for each argument qualifies its presence and identifies the clause in which the argument is defined.

Table 7 – Probe-submission Arguments

Argument	Presence	Clause
<i>Originator Argument</i>		
Originator-name	M	8.2.1.1.1.1
<i>Recipient Arguments</i>		
Recipient-name	M	8.2.1.1.1.2
Alternate-recipient-allowed	O	8.2.1.1.1.3
Recipient-reassignment-prohibited	O	8.2.1.1.1.4
Originator-requested-alternate-recipient	O	8.2.1.1.1.5
DL-expansion-prohibited	O	8.2.1.1.1.6
<i>Conversion Arguments</i>		
Implicit-conversion-prohibited	O	8.2.1.1.1.9
Conversion-with-loss-prohibited	O	8.2.1.1.1.10
Explicit-conversion	O	8.2.1.1.1.11
<i>Delivery Method Argument</i>		
Requested-delivery-method	O	8.2.1.1.1.14

Table 7 – Probe-submission Arguments

Argument	Presence	Clause
<i>Physical Delivery Argument</i>		
Physical-rendition-attributes	O	8.2.1.1.1.20
<i>Report Request Argument</i>		
Originator-report-request	M	8.2.1.1.1.22
<i>Security Arguments</i>		
Originator-certificate	O	8.2.1.1.1.25
Probe-origin-authentication-check	O	8.2.1.2.1.1
Message-security-label	O	8.2.1.1.1.30
<i>Content Arguments</i>		
Original-encoded-information-types	O	8.2.1.1.1.33
Content-type	M	8.2.1.1.1.34
Content-identifier	O	8.2.1.1.1.35
Content-correlator	O	8.2.1.1.1.36
Content-length	O	8.2.1.2.1.2
Notification-type	O	8.2.1.1.1.38
Service-message	O	8.2.1.1.1.39

8.2.1.2.1.1 Probe-origin-authentication-check

This argument provides any MTA through which the probe is transferred, with a means of authenticating the origin of the probe (to provide the Probe Origin Authentication element-of-service as defined in ITU-T Rec. X.400 | ISO/IEC 10021-1). It may be generated by the originator of the probe.

The **probe-origin-authentication-check** provides proof of the origin of the probe (Probe Origin Authentication), and proof of association between the **message-security-label** and the **content-identifier** of the subject-message.

The **probe-origin-authentication-check** is computed using the algorithm identified by the **probe-origin-authentication-algorithm-identifier** (an **algorithm-identifier**).

The **probe-origin-authentication-check** contains the **probe-origin-authentication-algorithm-identifier**, and an asymmetrically-encrypted hashed version of: the **probe-origin-authentication-algorithm-identifier**; and the **content-identifier** and **message-security-label** of the subject-message. Optional components are included in the **probe-origin-authentication-check** if they are present in the probe.

The **probe-origin-authentication-check** may be computed by the originator of the probe using the originator's secret-asymmetric-encryption-key. The **probe-origin-authentication-check** may be validated by any MTA through which the probe is transferred, using the public-asymmetric-encryption-key (**subject-public-key**) of the originator of the probe derived from the **originator-certificate**.

Addenda or future versions of this Recommendation | International Standard may define other forms of **probe-origin-authentication-check** (e.g., based on symmetric-encryption-techniques) which may be used by MTAs through which the probe is transferred to authenticate the origin of the probe.

8.2.1.2.1.2 Content-length

This argument specifies the length, in octets, of the **content** of the subject-message. It may be generated by the originator of the probe.

8.2.1.2.2 Results

Table 8 lists the results of the Probe-submission abstract-operation, and for each result qualifies its presence and identifies the clause in which the result is defined.

Table 8 – Probe-submission Results

Result	Presence	Clause
Probe-submission-identifier	M	8.2.1.2.2.1
Probe-submission-time	M	8.2.1.2.2.2
Content-identifier	C	8.2.1.1.1.35

8.2.1.2.2.1 Probe-submission-identifier

This result contains an **MTS-identifier** that uniquely and unambiguously identifies the probe-submission. It shall be generated by the MTS.

The MTS provides the **probe-submission-identifier** when notifying the MTS-user, via the Report-delivery abstract-operation, of its ability or otherwise to deliver the subject-message.

8.2.1.2.2.2 Probe-submission-time

This result indicates the **Time** at which the MTS agreed to undertake the probe. It shall be generated by the MTS.

8.2.1.2.3 Abstract-errors

Table 9 lists the abstract-errors that may disrupt the Probe-submission abstract-operation, and for each abstract-error identifies the clause in which the abstract-error is defined.

Table 9 – Probe-submission Abstract-errors

Abstract-error	Clause
Submission-control-violated	8.2.2.1
Element-of-service-not-subscribed	8.2.2.2
Originator-invalid	8.2.2.4
Recipient-improperly-specified	8.2.2.5
Inconsistent-request	8.2.2.7
Security-error	8.2.2.8
Unsupported-critical-function	8.2.2.9
Remote-bind-error	8.2.2.10

8.2.1.3 Cancel-deferred-delivery

The Cancel-deferred-delivery abstract-operation enables an MTS-user to abort the deferred-delivery of a message previously submitted by that user via the Message-submission abstract-operation.

The MTS-user identifies the message whose delivery is to be cancelled by means of the **message-submission-identifier** returned by the MTS as a result of the previous invocation of the Message-submission abstract-operation.

The successful completion of the abstract-operation signifies that the MTS has cancelled the deferred-delivery of the message.

The disruption of the abstract-operation by an abstract-error indicates that the deferred-delivery cannot be cancelled. The deferred-delivery of a message cannot be cancelled if the message has already been progressed for delivery and/or transfer within the MTS. The MTS may refuse to cancel the deferred-delivery of a message, if the MTS provided the originator of the message with **proof-of-submission**.

8.2.1.3.1 Arguments

Table 10 lists the arguments of the Cancel-deferred-delivery abstract-operation, and for each argument qualifies its presence and identifies the clause in which the argument is defined.

Table 10 – Cancel-deferred-delivery Arguments

Argument	Presence	Clause
<i>Submission Argument</i>		
Message-submission-identifier	M	8.2.1.3.1.1

8.2.1.3.1.1 Message-submission-identifier

This argument contains the **message-submission-identifier** of the message whose deferred-delivery is to be cancelled. It shall be supplied by the MTS-user.

The **message-submission-identifier** (an **MTS-identifier**) is that returned by the MTS as a result of a previous invocation of the Message-submission abstract-operation (see 8.2.1.1.2.1), when the message was submitted for deferred-delivery.

8.2.1.3.2 Results

The Cancel-deferred-delivery abstract-operation returns an empty result as indication of success.

8.2.1.3.3 Abstract-errors

Table 11 lists the abstract-errors that may disrupt the Cancel-deferred-delivery abstract-operation, and for each abstract-error identifies the clause in which the abstract-error is defined.

Table 11 – Cancel-deferred-delivery Abstract-errors

Abstract-error	Clause
Deferred-delivery-cancellation-rejected	8.2.2.3
Message-submission-identifier-invalid	8.2.2.6
Remote-bind-error	8.2.2.10

8.2.1.4 Submission-control

The Submission-control abstract-operation enables the MTS to temporarily limit the submission-port abstract-operations that the MTS-user may invoke, and the messages that the MTS-user may submit to the MTS via the Message-submission abstract-operation.

The MTS-user should hold until a later time, rather than abandon, abstract-operations and messages presently forbidden.

The successful completion of the abstract-operation signifies that the specified controls are now in force. These controls supersede any previously in force, and remain in effect until the association is released or the MTS re-invokes the Submission-control abstract-operation.

The abstract-operation returns an indication of any abstract-operations that the MTS-user would invoke, or any message types that the MTS-user would submit, were it not for the prevailing controls.

8.2.1.4.1 Arguments

Table 12 lists the arguments of the Submission-control abstract-operation, and for each argument qualifies its presence and identifies the clause in which the argument is defined.

Table 12 – Submission-control Arguments

Argument	Presence	Clause
<i>Submission Control Arguments</i>		
Restrict	O	8.2.1.4.1.1
Permissible-operations	O	8.2.1.4.1.2
Permissible-lowest-priority	O	8.2.1.4.1.3
Permissible-maximum-content-length	O	8.2.1.4.1.4
Permissible-security-context	O	8.2.1.4.1.5

8.2.1.4.1.1 Restrict

This argument indicates whether the controls on submission-port abstract-operations are to be updated or removed. It may be generated by the MTS.

This argument may have one of the following values:

update: the other arguments update the prevailing controls;

remove: all controls are to be removed; the other arguments are to be ignored.

In the absence of this argument, the default **update** shall be assumed.

8.2.1.4.1.2 Permissible-operations

This argument indicates the abstract-operations that the MTS-user may invoke on the MTS. It may be generated by the MTS.

This argument may have the value **allowed** or **prohibited** for each of the following:

message-submission: the MTS-user may/may not invoke the Message-submission abstract-operation; and

probe-submission: the MTS-user may/may not invoke the Probe-submission abstract-operation.

Other submission-port abstract-operations are not subject to controls, and may be invoked at any time.

In the absence of this argument, the abstract-operations that the MTS-user may invoke on the MTS are unchanged. If no previous controls are in force, the MTS-user may invoke both the Message-submission abstract-operation and the Probe-submission abstract-operation.

8.2.1.4.1.3 Permissible-lowest-priority

This argument contains the **priority** of the lowest priority message that the MTS-user shall submit to the MTS via the Message-submission abstract-operation. It may be generated by the MTS.

This argument may have one of the following values of the **priority** argument of the Message-submission abstract-operation: **normal**, **non-urgent** or **urgent**.

In the absence of this argument, the **priority** of the lowest priority message that the MTS-user shall submit to the MTS is unchanged. If no previous controls are in force, the MTS-user may submit messages of any priority.

8.2.1.4.1.4 Permissible-maximum-content-length

This argument contains the **content-length**, in octets, of the longest-content message that the MTS-user shall submit to the MTS via the Message-submission abstract-operation. It may be generated by the MTS.

In the absence of this argument, the **permissible-maximum-content-length** of a message that the MTS-user may submit to the MTS is unchanged. If no previous controls are in force, the content length is not explicitly limited.

8.2.1.4.1.5 Permissible-security-context

This argument temporarily limits the sensitivity of submission-port abstract-operations (submission-security-context) that the MTS-user may invoke on the MTS. It is a temporary restriction of the **security-context** established when the association was initiated (see 8.1.1.1.1.3). It may be generated by the MTS.

The **permissible-security-context** comprises one or more **security-labels** from the set of **security-labels** established as the **security-context** when the association was established.

In the absence of this argument, the **security-context** of submission-port abstract-operations is unchanged.

8.2.1.4.2 Results

Table 13 lists the results of the Submission-control abstract-operation, and for each result qualifies its presence and identifies the clause in which the result is defined.

Table 13 – Submission-control Results

Result	Presence	Clause
<i>"Waiting" Results</i>		
Waiting-operations	O	8.2.1.4.2.1
Waiting-messages	O	8.2.1.4.2.2
Waiting-encoded-information-types	O	8.2.1.4.2.3
Waiting-content-types	O	8.2.1.4.2.4

8.2.1.4.2.1 Waiting-operations

This result indicates the abstract-operations being held by the MTS-user, and that the MTS-user would invoke on the MTS if it were not for the prevailing controls. It may be generated by the MTS-user.

This result may have the value **holding** or **not-holding** for each of the following:

message-submission: the MTS-user is/is not holding messages, and would invoke the Message-submission abstract-operation on the MTS if it were not for the prevailing controls; and

probe-submission: the MTS-user is/is not holding probes, and would invoke the Probe-submission abstract-operation on the MTS if it were not for the prevailing controls.

In the absence of this result, it may be assumed that the MTS-user is not holding any messages or probes for submission to the MTS due to the prevailing controls.

8.2.1.4.2.2 Waiting-messages

This result indicates the kind of messages the MTS-user is holding for submission to the MTS, and would submit via the Message-submission abstract-operation, if it were not for the prevailing controls. It may be generated by the MTS-user.

This result may have one or more of the following values:

long-content: the MTS-user has messages held for submission to the MTS which exceed the **permissible-maximum-content-length** control currently in force;

low-priority: the MTS-user has messages held for submission to the MTS of a lower **priority** than the **permissible-lowest-priority** control currently in force;

other-security-labels: the MTS-user has messages held for submission to the MTS bearing **message-security-labels** other than those permitted by the current security-context.

In the absence of this result, it may be assumed that the MTS-user is not holding any messages or probes for submission to the MTS due to the **permissible-maximum-content-length**, **permissible-lowest-priority** or **permissible-security-context** controls currently in force.

8.2.1.4.2.3 Waiting-encoded-information-types

This result indicates the **encoded-information-types** in the **content** of any messages held by the MTS-user for submission to the MTS due to prevailing controls. It may be generated by the MTS-user.

In the absence of this result, the **encoded-information-types** of any messages held by the MTS-user for submission to the MTS are **unspecified**.

8.2.1.4.2.4 Waiting-content-types

This result indicates the **content-types** of any messages held by the MTS-user for submission to the MTS due to prevailing controls. It may be generated by the MTS-user.

In the absence of this result, the **content-types** of any messages held by the MTS-user for submission to the MTS are **unspecified**.

8.2.1.4.3 Abstract-errors

Table 14 lists the abstract-errors that may disrupt the Submission-control abstract-operation, and for each abstract-error identifies the clause in which the abstract-error is defined.

Table 14 – Submission-control Abstract-errors

Abstract-error	Clause
Security-error	8.2.2.8
Remote-bind-error	8.2.2.10

8.2.2 Abstract-errors

This clause defines the following submission-port abstract-errors:

- a) Submission-control-violated
- b) Element-of-service-not-subscribed
- c) Deferred-delivery-cancellation-rejected
- d) Originator-invalid
- e) Recipient-improperly-specified
- f) Message-submission-identifier-invalid
- g) Inconsistent-request
- h) Security-error
- i) Unsupported-critical-function
- j) Remote-bind-error.

8.2.2.1 Submission-control-violated

The Submission-control-violated abstract-error reports the violation by the MTS-user of a control on submission-port services imposed by the MTS via the Submission-control service.

The Submission-control-violated abstract-error has no parameters.

8.2.2.2 Element-of-service-not-subscribed

The Element-of-service-not-subscribed service reports that the requested abstract-operation cannot be provided by the MTS because the MTS-user has not subscribed to one of the elements-of-service the request requires.

The Element-of-service-not-subscribed abstract-error has no parameters.

8.2.2.3 Deferred-delivery-cancellation-rejected

The Deferred-delivery-cancellation-rejected abstract-error reports that the MTS cannot cancel the deferred-delivery of a message, either because the message has already been progressed for transfer and/or delivery, or because the MTS had provided the originator with **proof-of-submission**.

The Deferred-delivery-cancellation-rejected abstract-error has no parameters.

8.2.2.4 Originator-invalid

The Originator-invalid abstract-error reports that the message or probe cannot be submitted because the originator is incorrectly identified.

The Originator-invalid abstract-error has no parameters.

8.2.2.5 Recipient-improperly-specified

The Recipient-improperly-specified abstract-error reports that the message or probe cannot be submitted because one or more recipients are improperly specified.

The Recipient-improperly-specified abstract-error has the following parameters, generated by the MTS:

improperly-specified-recipients: the improperly specified **recipient-name(s)**.

8.2.2.6 Message-submission-identifier-invalid

The Message-submission-identifier-invalid abstract-error reports that the deferred-delivery of a message cannot be cancelled because the specified **message-submission-identifier** is invalid, or identifies a message submitted by another MTS-user.

The Message-submission-identifier-invalid abstract-error has no parameters.

8.2.2.7 Inconsistent-request

The Inconsistent-request abstract-error reports that the requested abstract-operation cannot be provided by the MTS because the MTS-user has made an inconsistent request.

The Inconsistent-request abstract-error has no parameters.

8.2.2.8 Security-error

The Security-error abstract-error reports that the requested abstract-operation could not be provided by the MTS or MTS-user because it would violate the security-policy in force.

The Security-error abstract-error has the following parameters:

security-problem: an identifier for the cause of the violation of the security-policy.

The use of the following security-error codes is dependent on the security-policy and the implementation of security functions. In particular, these security-error codes may be used by a pervasive security monitor function, which monitors the routine operation of a UA, MS or MTA and ensures that the security-policy is not violated by the normal operation of the MHS component.

The **security-problem** parameter may have one of the following values for the Message-submission or Probe-submission abstract-operations:

- a) The following values indicate a security violation by the user:

security-policy-violation: the security-policy is violated;

security-services-refusal: the security services requested cannot be supported;

unauthorised-dl-name: the recipient MTS-user OR-name identifies a DL whose use is unauthorised for security reasons;

NOTE – If the MTA is unable to determine that the OR-name identifies a DL then the value unauthorised-recipient-name may be used instead.

unauthorised-originator-name: the originator MTS-user OR-name is unauthorised for security reasons;

unauthorised-recipient-name: the recipient MTS-user OR-name is unauthorised for security reasons;

unknown-security-label: the security policy identifier in the message security label is not recognised by the MTA. Such a policy is not supported by the MTA.

- b) The following values indicate an error within the security system:

invalid-security-label: the security policy identifier in the message security label identifies a policy which is known to the MTA, but which is not acceptable to that system;

mandatory-parameter-absence: a mandated security element for compliance with the security-policy in force is absent;

operation-security-failure: the submission operation failed for security reasons;

security-context-failure: the message security label is incompatible with the security-context in force.

The security-problem parameter may have one of the following values for the Submission-control abstract-operation:

- a) The following values indicate a security violation by the user:

security-policy-violation: the security-policy is violated;

security-services-refusal: the security services requested cannot be supported.

- b) The following values indicate an error within the security system:

incompatible-change-with-original-security-context: the proposed permissible-security-context is not a subset of the original security-context;

mandatory-parameter-absence: a mandated security element for compliance with the security-policy in force is absent;

operation-security-failure: the Submission-control operation failed for security reasons.

8.2.2.9 Unsupported-critical-function

The Unsupported-critical-function abstract-error reports that an argument of the abstract-operation was marked as **critical-for-submission** (see 9.2) but is unsupported by the MTS.

The Unsupported-critical-function abstract-error has no parameters.

8.2.2.10 Remote-bind-error

The Remote-bind-error abstract-error reports that the requested abstract-operation cannot be provided by the MS because the MS is unable to bind to the MTS, or because there is no association in existence between the MS and the UA. This abstract-error occurs on an indirect submission to the MTS via an MS, or on invocation by the MTS of a submission-control abstract-operation via an MS.

The Remote-bind-error abstract-error has no parameters.

8.3 Delivery Port

This clause defines the abstract-operations and abstract-errors which occur at a delivery-port.

8.3.1 Abstract-operations

This clause defines the following delivery-port abstract-operations:

- a) Message-delivery
- b) Report-delivery
- c) Delivery-Control.

8.3.1.1 Message-delivery

The Message-delivery abstract-operation enables the MTS to deliver a message to an MTS-user.

The MTS-user shall not refuse delivery of a message unless the delivery would violate the Delivery-control restrictions then in force.

8.3.1.1.1 Arguments

Table 15 lists the arguments of the Message-delivery abstract-operation, and for each argument qualifies its presence and identifies the clause in which the argument is defined.

Table 15 – Message-delivery Arguments

Argument	Presence	Clause
<i>Delivery Arguments</i>		
Message-delivery-identifier	M	8.3.1.1.1.1
Message-delivery-time	M	8.3.1.1.1.2
Message-submission-time	M	8.2.1.1.2.2
Trace-information	O	12.2.1.1.1.3
Internal-trace-information	O	12.2.1.1.1.4
<i>Originator Argument</i>		
Originator-name	M	8.2.1.1.1.1
<i>Recipient Arguments</i>		
This-recipient-name	M	8.3.1.1.1.3
Originally-intended-recipient-name	C	8.3.1.1.1.4
Redirection-history	C	8.3.1.1.1.5
Other-recipient-names	C	8.3.1.1.1.6
DL-expansion-history	C	8.3.1.1.1.7
DL-exempted-recipients	O	8.2.1.1.1.40
<i>Priority Argument</i>		
Priority	C	8.2.1.1.1.8
<i>Conversion Arguments</i>		
Implicit-conversion-prohibited	C	8.2.1.1.1.9
Conversion-with-loss-prohibited	C	8.2.1.1.1.10
Converted-encoded-information-types	C	8.3.1.1.1.8
<i>Delivery Method Argument</i>		
Requested-delivery-method	C	8.2.1.1.1.14

Table 15 – Message-delivery Arguments

Argument	Presence	Clause
<i>Physical Delivery Arguments</i>		
Physical-forwarding-prohibited	C*	8.2.1.1.1.15
Physical-forwarding-address-request	C*	8.2.1.1.1.16
Physical-delivery-modes	C*	8.2.1.1.1.17
Registered-mail-type	C*	8.2.1.1.1.18
Recipient-number-for-advice	C*	8.2.1.1.1.19
Physical-rendition-attributes	C*	8.2.1.1.1.20
Originator-return-address	C*	8.2.1.1.1.21
Physical-delivery-report-request	C*	8.2.1.1.1.24
<i>Security Arguments</i>		
Originator-certificate	C	8.2.1.1.1.25
Message-token	C	8.2.1.1.1.26
Content-confidentiality-algorithm-identifier	C	8.2.1.1.1.27
Content-integrity-check	C	8.2.1.1.1.28
Message-origin-authentication-check	C	8.2.1.1.1.29
Message-security-label	C	8.2.1.1.1.30
Proof-of-delivery-request	C	8.2.1.1.1.32
Multiple-originator-certificates	O	8.2.1.1.1.41
Recipient-certificate	O	8.2.1.1.1.42
Certificate-selectors	O	8.2.1.1.1.43
Certificate-selectors-override	O	8.2.1.1.1.44
<i>Content Arguments</i>		
Original-encoded-information-types	C	8.2.1.1.1.33
Content-type	M	8.2.1.1.1.34
Content-identifier	C	8.2.1.1.1.35
Content	M	8.2.1.1.1.37

NOTE – C* indicates that these arguments are normally absent for non-PD-recipients but may appear in special cases (e.g. redirection).

8.3.1.1.1.1 Message-delivery-identifier

This argument contains an **MTS-identifier** that distinguishes the message from all other messages at the delivery-port. It shall be generated by the MTS, and shall have the same value as the **message-submission-identifier** supplied to the originator of the message when the message was submitted.

8.3.1.1.1.2 Message-delivery-time

This argument contains the **Time** at which delivery occurs and at which the MTS is relinquishing responsibility for the message. It shall be generated by the MTS.

In the case of physical delivery, this argument indicates the **Time** at which the PDAU has taken responsibility for printing and further delivery of the message.

The value of this argument shall be the same as the value of the **message-delivery-time** argument reported to the originator of the message (see 8.3.1.2.1.9) in a delivery-report.

8.3.1.1.1.3 This-recipient-name

This argument contains the **OR-name** of the recipient to whom the message is being delivered. It shall be generated by the MTS.

The value of this argument shall be the same as the corresponding value of the **recipient-name** argument (i.e., the one that caused the message to be delivered to this recipient) which was present in the message immediately prior to delivery.

The **this-recipient-name** contains the **OR-name** of the individual recipient, i.e., shall not contain the **OR-name** of a DL.

The **OR-name** of the intended-recipient (if different, and the message has been redirected or DL-expanded) is contained in the **originally-intended-recipient-name** argument.

8.3.1.1.1.4 Originally-intended-recipient-name

This argument contains the **OR-name** of the recipient specified by the originator at the time of submission, as modified by the message-submission procedure (see 14.6.1). It shall be generated by the MTS (at the MTA performing message-delivery or report-generation) if the originally-specified **OR-name** of the recipient has been replaced as a result of DL-expansion or redirection.

8.3.1.1.1.5 Redirection-history

This argument documents the redirection events which have occurred during the transfer of the message through the MTS. It shall be generated by the MTS if redirection has occurred. For each redirection event that has occurred, it contains the **OR-name** of the intended recipient prior to the redirection, the **time** at which redirection occurred, and the reason for the redirection.

The **redirection-reason** has one of the following values:

recipient-assigned-alternate-recipient: the intended-recipient of the message requested that the message be redirected to a **recipient-assigned-alternate-recipient**; the originator of the message did not prohibit recipient-reassignment (see 8.2.1.1.1.4); the MTS redirected the message to the **recipient-assigned-alternate-recipient**;

originator-requested-alternate-recipient: the message could not be delivered to the intended-recipient or **recipient-assigned-alternate-recipient** (if registered); the **originator-requested-alternate-recipient** argument identified an alternate-recipient requested by the originator of the message; the MTS redirected the message to the **originator-requested-alternate-recipient**;

recipient-MD-assigned-alternate-recipient: the **recipient-name** argument did not identify a recipient MTS-user; the **alternate-recipient-allowed** argument generated by the originator of the message allowed delivery to an alternate-recipient; the MTS redirected the message to an alternate-recipient assigned by the recipient-MD to receive such messages;

directory-look-up: the **OR-address** of the intended-recipient did not identify a recipient MTS-user; the **OR-name** of that intended-recipient also contained a **directory-name** which was used to obtain from the Directory a different **OR-address** for that intended-recipient; the MTS redirected the message to the replacement **OR-address** for that intended-recipient.

alias: the **recipient-name** argument did not contain a preferred address of the specified MTS-user; the MTS redirected the message to a preferred address of that MTS-user.

NOTE 1 – The distinction between preferred and non-preferred addresses is established by local configuration.

Some systems conforming to earlier versions of this Specification may not support the values **alias** or **directory-look-up**. These values shall not be transmitted to systems that do not support them, except by bilateral agreement.

NOTE 2 – In order to achieve this, it is recommended that MTA implementations intended for use at the boundary between old and new systems (e.g., at domain boundaries) be provided with a configurable facility to modify the **redirection-history**. This facility would replace **alias** by **recipient-assigned-alternate-recipient** or replace **directory-look-up** by **originator-assigned-alternate-recipient** as required when transferring to specified adjacent MTAs.

8.3.1.1.1.6 Other-recipient-names

If the originator of the message requested disclosure of other recipients, this argument contains the **OR-names** of the originally-specified recipients other than the one (if any) identified by either the **originally-intended-recipient-name** argument, if present, or else by the **this-recipient-name** argument. This argument shall be generated by the MTS if, and only if, the message-submission abstract-operation had the **disclosure-of-other-recipients** argument set to **disclosure-of-other-recipients-requested** and there is at least one such other recipient.

Each **other-recipient-name** contains the **OR-name** of an individual recipient or a DL.

NOTE – If DL expansion has been performed, the **OR-names** of the DL's members are not disclosed. The **OR-name** of the DL is disclosed if, and only if, it is that of an originally-specified recipient.

8.3.1.1.1.7 DL-expansion-history

This argument contains the sequence of **OR-names** of any DLs which have been expanded to add recipients to the copy of the message delivered to the recipient and the **Time** of each expansion. It shall be generated by the MTS if any DL-expansion has occurred.

8.3.1.1.1.8 Converted-encoded-information-types

This argument identifies the **encoded-information-types** of the message **content** after conversion, if conversion took place. It may be generated by the MTS.

8.3.1.1.2 Results

Table 16 lists the results of the Message-delivery abstract-operation, and for each result qualifies its presence and identifies the clause in which the result is defined.

Table 16 – Message-delivery Results

Result	Presence	Clause
<i>Proof of Delivery Results</i>		
Recipient-certificate	O	8.3.1.1.2.1
Proof-of-delivery	C	8.3.1.1.2.2

8.3.1.1.2.1 Recipient-certificate

This argument contains the **certificate** of the recipient of the message. It shall be generated by a trusted source (e.g., a certification-authority), and may be supplied by the recipient of the message, if the originator of the message requested **proof-of-delivery** (see 8.2.1.1.1.32) and an asymmetric-encryption-algorithm is used to compute the **proof-of-delivery**.

The **recipient-certificate** may be used to convey a verified copy of the public-asymmetric-encryption-key (**subject-public-key**) of the recipient of the message.

The recipient's public-asymmetric-encryption-key may be used by the originator of the message to validate the **proof-of-delivery**.

8.3.1.1.2.2 Proof-of-delivery

This argument provides the originator of the message with proof that the message has been delivered to the recipient (to provide the Proof of Delivery element-of-service as defined in ITU-T Rec. X.400 | ISO/IEC 10021-1). Depending on the encryption-algorithm used and the security-policy in force, this argument may also provide the Non Repudiation of Delivery element-of-service (as defined in ITU-T Rec. X.400 | ISO/IEC 10021-1). It shall be generated by the recipient of the message, if the originator of the message requested **proof-of-delivery** (see 8.2.1.1.1.32).

The **proof-of-delivery** is computed using the algorithm identified by the **proof-of-delivery-algorithm-identifier** (an **algorithm-identifier**).

The **proof-of-delivery** contains the **proof-of-delivery-algorithm-identifier**, and an encrypted function (e.g., a compressed or hashed version) of the **proof-of-delivery-algorithm-identifier**, the **delivery-time**, and the **this-recipient-name**, the **originally-intended-recipient-name**, the message **content**, the **content-identifier**, and the **message-security-label** of the delivered message. Optional components are included in the **proof-of-delivery** if they are present in the delivered message. The **proof-of-delivery** is computed using the message **content** as delivered (i.e. either unencrypted or encrypted).

Receipt of this argument provides the originator of the message with Proof of Delivery of the message to the recipient. Non-receipt of this argument provides neither Proof of Delivery nor proof of non-delivery (unless a secure route and trusted functionality are employed).

If an asymmetric-encryption-algorithm is used, the **proof-of-delivery** may be computed by the recipient of the message using the recipient's secret-asymmetric-encryption-key. The originator of the message may validate the **proof-of-delivery** using the recipient's public-asymmetric-encryption-key (**subject-public-key**) derived from the **recipient-certificate**. An asymmetric **proof-of-delivery** may also provide for Non Repudiation of Delivery subject to availability of an appropriate Public Key infrastructure.

If a symmetric-algorithm is used, a symmetric-encryption-key is used by the recipient to compute the **proof-of-delivery**, and by the originator to validate the **proof-of-delivery**. If a symmetric-encryption-algorithm is used then the **proof-of-delivery** can only provide Non Repudiation of Delivery if the security-policy in force provides for the

involvement of a third party acting as a notary. The means by which the symmetric-encryption-key is distributed is not currently defined by this Service Definition.

8.3.1.1.3 Abstract-errors

Table 17 lists the abstract-errors that may disrupt the Message-delivery abstract-operation, and for each abstract-error identifies the clause in which the abstract-error is defined.

Table 17 – Message-delivery Abstract-errors

Abstract-error	Clause
Delivery-control-violated	8.3.2.1
Security-error	8.3.2.3
Unsupported-critical-function	8.3.2.4

8.3.1.2 Report-delivery

The **Report-delivery** abstract-operation enables the MTS to acknowledge to the MTS-user one or more outcomes of a previous invocation of the Message-submission or Probe-submission abstract-operations.

For the Message-submission abstract-operation, the Report-delivery abstract-operation indicates the delivery or non-delivery of the submitted message to one or more recipients.

For the Probe-submission abstract-operation, the Report-delivery abstract-operation indicates whether or not a message could be delivered, or a DL-expansion could occur, if the message were to be submitted.

A single invocation of the Message-submission or Probe-submission abstract-operation may provoke several occurrences of the Report-delivery abstract-operation, each covering one or more intended recipients. A single occurrence of the Report-delivery abstract-operation may report on both delivery and non-delivery to different recipients.

An invocation of the Message-submission or Probe-submission abstract-operation by one MTS-user may provoke occurrences of the Report-delivery abstract-operation to another MTS-user, i.e., reports delivered to the owner of a DL.

The MTS-user shall not refuse to accept the delivery of a report unless the delivery of the report would violate the Delivery-control restrictions then in force.

8.3.1.2.1 Arguments

Table 18 lists the arguments of the Report-delivery abstract-operation, and for each argument qualifies its presence and identifies the clause in which the argument is defined.

Table 18 – Report-delivery Arguments

Argument	Presence	Clause
<i>Subject Submission Argument</i>		
Subject-submission-identifier	M	8.3.1.2.1.1
<i>Recipient Arguments</i>		
Actual-recipient-name	M	8.3.1.2.1.2
Originally-intended-recipient-name	C	8.3.1.1.1.4
Redirection-history	C	8.3.1.1.1.5
Originator-and-DL-expansion-history	C	8.3.1.2.1.3
Reporting-DL-name	C	8.3.1.2.1.4
<i>Report Envelope Arguments</i>		
Redirection-history	C	8.3.1.2.1.5
Trace-information	O	12.2.1.1.1.3
Internal-trace-information	O	12.2.1.1.1.4
Reporting-MTA-name	C	8.3.1.2.1.17
<i>Conversion Arguments</i>		
Converted-encoded-information-types	C	8.3.1.2.1.6

Table 18 – Report-delivery Arguments

Argument	Presence	Clause
<i>Supplementary Information Arguments</i>		
Supplementary-information	C	8.3.1.2.1.7
Physical-forwarding-address	C	8.3.1.2.1.8
<i>Delivery Arguments</i>		
Message-delivery-time	C	8.3.1.2.1.9
Type-of-MTS-user	C	8.3.1.2.1.10
<i>Non-delivery Arguments</i>		
Non-delivery-reason-code	C	8.3.1.2.1.11
Non-delivery-diagnostic-code	C	8.3.1.2.1.12
<i>Security Arguments</i>		
Recipient-certificate	C	8.3.1.1.2.1
Proof-of-delivery	C	8.3.1.1.2.2
Reporting-MTA-certificate	C	8.3.1.2.1.13
Report-origin-authentication-check	C	8.3.1.2.1.14
Message-security-label	C	8.2.1.1.1.30
<i>Content Arguments</i>		
Original-encoded-information-types	C	8.2.1.1.1.33
Content-type	C	8.3.1.2.1.15
Content-identifier	C	8.2.1.1.1.35
Content-correlator	C	8.2.1.1.1.36
Returned-content	C	8.3.1.2.1.16

8.3.1.2.1.1 Subject-submission-identifier

This argument contains the **message-submission-identifier** or the **probe-submission-identifier** of the subject of the report. It shall be supplied by the MTS.

8.3.1.2.1.2 Actual-recipient-name

This argument contains the **OR-name** of a recipient of the message. It shall be generated by the originator of the message, or by the MTS if the message has been redirected or DL-expanded. A different value of this argument shall be specified for each recipient of the subject to which this report relates.

In the case of a delivery report, the **actual-recipient-name** is the name of the actual recipient of the message, and has the same value as the **this-recipient-name** argument of the delivered message. In the case of a non-delivery-report, the **actual-recipient-name** is the **OR-name** of the recipient to which the message was being directed when the reason for non-delivery was encountered.

The **actual-recipient-name** may be an originally-specified **recipient-name**, or the **OR-name** of a replacement recipient to which the message has been redirected, or the **OR-name** of a DL-member if the message has been DL-expanded. If the message has been redirected or DL-expanded, the **OR-name** of the originally-specified recipient is contained in the **originally-intended-recipient-name** argument.

The **actual-recipient-name** contains the **OR-name** of an individual recipient or DL.

8.3.1.2.1.3 Originator-and-DL-expansion-history

This argument contains a sequence of **OR-names** and associated times which document the history of the origin of the subject-message. The first **OR-name** in the sequence is the **OR-name** of the originator of the subject, and the remainder of the sequence is a sequence of **OR-names** of the DLs that have been expanded in directing the subject towards the recipient (the latter being the same as the **DL-expansion-history**). It shall be generated by the originating-MTA of the report if any DL-expansion has occurred on the subject.

The **originator-and-DL-expansion-history** contains the **OR-name** of the originator of the subject and each DL, and the **Time** at which the associated event occurred.

8.3.1.2.1.4 Reporting-DL-name

This argument contains the **OR-name** of the DL that forwarded the report to the owner of the DL. It shall be generated by a DL-expansion-point (an MTA) when forwarding a report to the owner of the DL, in line with the reporting-policy of the DL.

The **reporting-DL-name** contains the **OR-name** of the DL forwarding the report.

8.3.1.2.1.5 Redirection-history

This argument documents the redirection events which have occurred during the transfer of the report through the MTS. It shall be generated by the MTS if redirection of the report has occurred. For each redirection event that has occurred, it contains the **report-destination-name** prior to the redirection, the **time** at which redirection occurred, and the reason for the redirection. The values for **redirection-reason** are defined in 8.3.1.1.1.5, except that **originator-requested-alternate-recipient** is not applicable to reports.

NOTE – In Table 18 the Recipient Argument Redirection-history contains the Redirection-history of the subject of the report, whereas the Report Envelope Argument Redirection-history contains the Redirection-history of the report itself.

8.3.1.2.1.6 Converted-encoded-information-types

This argument identifies the **encoded-information-types** of the subject-message **content** after conversion, if conversion took place. For a report on a message, this argument indicates the actual **encoded-information-types** of the converted message **content**. For a report on a probe, this argument indicates the **encoded-information-types** the subject-message **content** would have contained after conversion, if the subject-message were to have been submitted. It may be generated by the MTS. A different value of this parameter may be specified for each recipient of the subject to which the report relates.

8.3.1.2.1.7 Supplementary-information

This argument may contain information supplied by the originator of the report, as a printable string. It may be generated by the originating-MTA of the report or an associated access-unit. A different value of this argument may be specified for each intended recipient of the subject to which the report relates.

Supplementary-information may be used by a Teletex-access-unit or a Teletex/Telex conversion facility. It may contain a Received Answer-back, Telex Transmission Duration, or Note and Received Recorded Message as a printable string.

Supplementary-information may also be used by other access-units, or by the originating-MTA of the report itself, to convey printable information to the originator of the message.

8.3.1.2.1.8 Physical-forwarding-address

This argument contains the new **postal-OR-address** of the physical-recipient of the message. It may be generated by the associated PDAU of the originating-MTA of the report, if the originator of the message requested the physical-forwarding-address of the recipient (see 8.2.1.1.1.16). A different value of this argument may be specified for each intended recipient of the subject-message to which the report relates.

8.3.1.2.1.9 Message-delivery-time

This argument contains the **Time** at which the subject-message was (or would have been) delivered to the recipient MTS-user. It shall be generated by the MTS if the message was (or would have been) successfully delivered. A different value of this argument may be specified for each intended-recipient of the subject to which the report relates.

In the case of physical delivery, this argument indicates the **Time** at which the PDAU has taken responsibility for printing and further delivery of the message.

If the subject-message was delivered, the value of this argument shall be the same as the value of the **message-delivery-time** argument of the delivered message (see 8.3.1.1.1.2).

8.3.1.2.1.10 Type-of-MTS-user

This argument indicates the type of recipient MTS-user to which the message was (or would have been) delivered. It shall be generated by the MTS if the message was (or would have been) successfully delivered. A different value of this argument may be specified for each intended-recipient of the subject to which the report relates.

This argument may have one of the following values:

public: a UA owned by an Administration;

private: a UA owned by other than an Administration;

ms: a message-store;
DL: a distribution-list;
PDAU: a physical-delivery-access-unit (PDAU);
physical-recipient: a physical-recipient of a PDS;
other: an access-unit of another kind.

8.3.1.2.1.11 Non-delivery-reason-code

This argument contains a code indicating the reason the delivery of the subject-message failed (or, in the case of a probe, would have failed). It shall be generated by the MTS if the message was (or would have been) unsuccessfully delivered. A different value of this argument may be specified for each intended-recipient of the subject to which the report relates.

This argument may have one of the following values:

transfer-failure: indicates that, while the MTS was attempting to deliver or probe delivery of the subject-message, some communication failure prevented it from doing so;
unable-to-transfer: indicates that, due to some problem with the subject itself, the MTS could not deliver or probe delivery of the subject-message;
conversion-not-performed: indicates that a conversion necessary for the delivery of the subject-message was (or would be) unable to be performed;
physical-rendition-not-performed: indicates that the PDAU was unable to physically render the subject-message;
physical-delivery-not-performed: indicates that the PDS was unable to physically deliver the subject-message;
restricted-delivery: indicates that the recipient subscribes to the restricted-delivery element-of-service (as defined in ITU-T Rec. X.400 | ISO/IEC 10021-1) which prevented (or would prevent) the delivery of the subject-message;
directory-operation-unsuccessful: indicates that the outcome of a required Directory operation was unsuccessful;
deferred-delivery-not-performed: indicates that a request for deferred delivery of the subject-message was unable to be performed;
transfer-failure-for-security-reason: indicates that, while the MTS was attempting to deliver or probe delivery of the subject-message, a security failure prevented it from doing so.

Other **non-delivery-reason-codes** may be specified in addenda or future versions of this Recommendation | International Standard.

Further information on the nature of the problem preventing delivery is contained in the **non-delivery-diagnostic-code** argument.

8.3.1.2.1.12 Non-delivery-diagnostic-code

This argument contains a code indicating the nature of the problem which caused delivery or probing of delivery of the subject-message, to fail. It may be generated by the MTS if the message was (or would have been) unsuccessfully delivered. A different value of this argument may be specified for each intended-recipient of the subject to which the report relates.

This argument may have one of the following values:

unrecognised-OR-name: the **recipient-name** argument of the subject does not contain an **OR-name** recognised by the MTS;
ambiguous-OR-name: the **recipient-name** argument of the subject identifies more than one potential recipient (i.e., is ambiguous);
MTS-congestion: the subject could not be progressed, due to congestion in the MTS;
loop-detected: the subject was detected looping within the MTS;
recipient-unavailable: the recipient MTS-user was (or would be) unavailable to take delivery of the subject-message;
maximum-time-expired: the maximum time for delivering the subject-message, or performing the subject-probe, expired;

encoded-information-types-unsupported: the encoded-information-types of the subject-message are unsupported by the recipient MTS-user;

content-too-long: the **content-length** of the subject-message is too long for the recipient MTS-user to take delivery (exceeds the deliverable-maximum-content-length);

conversion-impractical: a conversion required for the subject-message to be delivered is impractical;

implicit-conversion-prohibited: a conversion required for the subject-message to be delivered has been prohibited by the originator of the subject (see 8.2.1.1.1.9);

implicit-conversion-not-subscribed: a conversion required for the subject-message to be delivered has not been subscribed to by the recipient;

invalid-arguments: one or more arguments in the subject was detected as being invalid;

content-syntax-error: a syntax error was detected in the content of the subject-message (not applicable to subject-probes);

size-constraint-violation: indicates that the value of one or more parameters(s) of the subject violated the size constraints defined in this Service Definition, and that the MTS was not prepared to handle the specified value(s);

protocol-violation: indicates that one or more mandatory argument(s) were missing from the subject;

content-type-not-supported: indicates that processing of a **content-type** not supported by the MTS was (or would be) required to deliver the subject-message;

too-many-recipients: indicates that the MTS was (or would be) unable to deliver the subject-message due to the number of specified recipients of the subject-message (see 8.2.1.1.1.2);

no-bilateral-agreement: indicates that delivery of the subject-message required (or would require) a bilateral agreement where no such agreement exists;

unsupported-critical-function: indicates that a critical function required for the transfer or delivery of the subject-message was not supported by the originating-MTA of the report;

conversion-with-loss-prohibited: a conversion required for the subject-message to be delivered would have resulted in loss of information; conversion with loss of information was prohibited by the originator of the subject (see 8.2.1.1.1.10);

line-too-long: a conversion required for the subject-message to be delivered would have resulted in loss of information because the original line length was too long;

page-split: a conversion required for the subject-message to be delivered would have resulted in loss of information because an original page would be split;

pictorial-symbol-loss: a conversion required for the subject-message to be delivered would have resulted in loss of information because of a loss of one or more pictorial symbols;

punctuation-symbol-loss: a conversion required for the subject-message to be delivered would have resulted in loss of information because of a loss of one or more punctuation symbols;

alphabetic-character-loss: a conversion required for the subject-message to be delivered would have resulted in loss of information because of a loss of one or more alphabetic characters;

multiple-information-loss: a conversion required for the subject-message to be delivered would have resulted in multiple loss of information;

recipient-reassignment-prohibited: indicates that the MTS was (or would be) unable to deliver the subject-message because the originator of the subject prohibited redirection to a **recipient-assigned-alternate-recipient** (see 8.2.1.1.1.4);

redirection-loop-detected: the subject-message could not be redirected to a replacement recipient because that recipient had previously redirected the message (redirection-loop);

DL-expansion-prohibited: indicates that the MTS was (or would be) unable to deliver the subject-message because the originator of the subject prohibited the expansion of DLs (see 8.2.1.1.1.6);

no-DL-submit-permission: the originator of the subject (or the DL of which this DL is a member, in the case of nested DLs) does not have permission to submit messages to this DL;

DL-expansion-failure: indicates that the MTS was unable to complete the expansion of a DL;

physical-rendition-attributes-not-supported: the PDAU does not support the physical-rendition-attributes requested (see 8.2.1.1.1.20);

undeliverable-mail-physical-delivery-address-incorrect: the subject-message was undeliverable because the specified recipient **postal-OR-address** was incorrect;

undeliverable-mail-physical-delivery-office-incorrect-or-invalid: the subject-message was undeliverable because the physical-delivery-office identified by the specified recipient **postal-OR-address** was incorrect or invalid (does not exist);

undeliverable-mail-physical-delivery-address-incomplete: the subject-message was undeliverable because the specified recipient **postal-OR-address** was incompletely specified;

undeliverable-mail-recipient-unknown: the subject-message was undeliverable because the recipient specified in the recipient **postal-OR-address** was not known at that address;

undeliverable-mail-recipient-deceased: the subject-message was undeliverable because the recipient specified in the recipient **postal-OR-address** is deceased;

undeliverable-mail-organization-expired: the subject-message was undeliverable because the recipient organization specified in the recipient **postal-OR-address** has expired;

undeliverable-mail-recipient-refused-to-accept: the subject-message was undeliverable because the recipient specified in the recipient **postal-OR-address** refused to accept it;

undeliverable-mail-recipient-did-not-claim: the subject-message was undeliverable because the recipient specified in the recipient **postal-OR-address** did not collect the mail;

undeliverable-mail-recipient-changed-address-permanently: the subject-message was undeliverable because the recipient specified in the recipient **postal-OR-address** had changed address permanently ('moved'), and forwarding was not applicable;

undeliverable-mail-recipient-changed-address-temporarily: the subject-message was undeliverable because the recipient specified in the recipient **postal-OR-address** had changed address temporarily ('on travel'), and forwarding was not applicable;

undeliverable-mail-recipient-changed-temporary-address: the subject-message was undeliverable because the recipient specified in the recipient **postal-OR-address** had changed temporary address ('departed'), and forwarding was not applicable;

undeliverable-mail-new-address-unknown: the subject-message was undeliverable because the recipient has moved and the recipient's new address is unknown;

undeliverable-mail-recipient-did-not-want-forwarding: the subject-message was undeliverable because delivery would have required physical-forwarding which the recipient did not want;

undeliverable-mail-originator-prohibited-forwarding: the physical-forwarding required for the subject-message to be delivered has been prohibited by the originator of the subject-message (see 8.2.1.1.1.15);

secure-messaging-error: the subject could not be progressed because the message security label would violate the security-policy in force, which goes against the security context;

unable-to-downgrade: the subject could not be transferred because it could not be downgraded (see Annex B of ITU-T Rec. X.419 | ISO/IEC 10021-6);

unable-to-complete-transfer: receiving system has indicated that it is permanently unable to complete transfer of the subject; for example, when the transfer is of such a size that it could never be accepted;

transfer-attempts-limit-reached: the maximum number or time duration of repeat attempts to transfer the subject was reached;

incorrect-notification-type: the subject-message contained a **notification-type** argument which did not correspond to its **content**.

For security errors, this argument may have one of the following values:

- a) The following values indicate a security violation by the user:

DL-expansion-prohibited-by-security-policy: the subject-message was addressed to a DL, but the security policy prohibited expansion of that DL;

forbidden-alternate-recipient: the subject-message would have been redirected, but the new recipient is unacceptable for security reasons;

security-policy-violation: the security-policy is violated;

security-services-refusal: the security services requested cannot be supported;

unauthorised-DL-member: the DL-expansion was not performed because the MTA discovered that one of the members of the DL was prohibited by the security policy from receiving this message;

unauthorised-DL-name: The MTA has detected that the recipient OR-name identifies a DL but the local security policy does not permit the onward transfer towards the DL-expansion point;