INTERNATIONAL STANDARD

ISO/IEC 10021-4

Third edition
2003-12-15

Information technology — Message Handling Systems (MHS): Message transfer system — Abstract service definition and procedures

Technologies de l'information — Systèmes de messagerie (MHS): Système de transfert de messages — Définition et procédures du service abstrait

Reference number
ISO/IEC 10021-4:2003(E)

© ISO/IEC 2003

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

Not for Resale

PDF disclaimer

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

Adobe is a trademark of Adobe Systems Incorporated.

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

© ISO/IEC 2003

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

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

Published in Switzerland

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

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
	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

© ISO/IEC 2003 All rights reserved

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

Page

SECTION THREE – MESSAGE TRANSFER AGENT ABSTRACT SERVICE 102

10 Refined Message Transfer System Model 102

11 Message Transfer Agent Abstract Service Overview 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

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

Page
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

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

Foreword

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

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

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

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

ISO/IEC 10021-4 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 6, *Telecommunications and information exchange between systems,* in collaboration with ITU-T. The identical text is published as ITU-T Rec. X.411.

This third edition cancels and replaces the second edition (ISO/IEC 10021-4:1997), which has been technically revised. It also incorporates the Technical Corrigendum ISO/IEC 10021-4:1997/Cor. 1:1998.

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

— *Part 1: System and service overview*

— *Part 2: Overall architecture*

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

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

— *Part 6: Protocol specifications*

— *Part 7: Interpersonal messaging system*

— *Part 8: Electronic Data Interchange Messaging Service*

— *Part 9: Electronic Data Interchange Messaging System*

— *Part 10: MHS routing*

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

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

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.

© ISO/IEC 2003 All rights reserved

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

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

INTERNATIONAL STANDARD 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.

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

2.1 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 10021-1:2003, *Information technology – Message Handling Systems (MHS) – Part 1: System and service overview*.
- ITU-T Recommendation X.402 (1999) | ISO/IEC 10021-2:2003, *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 10021-6:2003, *Information technology – Message Handling Systems (MHS) – Protocol specifications*.
- ITU-T Recommendation X.420 (1999) | ISO/IEC 10021-7:2003, *Information technology – Message Handling Systems (MHS) – Interpersonal messaging system*.
- ITU-T Recommendation 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*.

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

– ITU-T Recommendation X.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 |

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

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.

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

The 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.

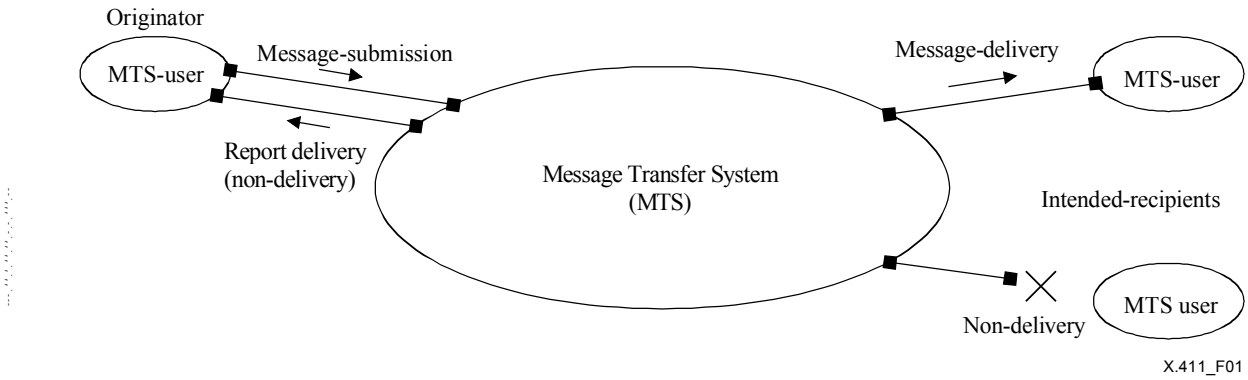


Figure 1 – Message Transfer System Model

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

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

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 it's **credentials** with the MTS, or the MTS to change it's **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.

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

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
Bind Arguments		
Initiator-name	M	8.1.1.1.1
Initiator-credentials	M	8.1.1.1.2
Security-context	O	8.1.1.1.3
Messages-waiting	O	8.1.1.1.4

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**.

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

The **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).

8.1.1.1.1.3 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.

8.1.1.1.1.4 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
Bind Results		
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.

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

If 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.

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

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.

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

The 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
Originator Argument		
Originator-name	M	8.2.1.1.1.1
Recipient Arguments		
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
Priority Argument		
Priority	O	8.2.1.1.1.8
Conversion Arguments		
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

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

Table 3 – Message-submission Arguments

Argument	Presence	Clause
Delivery Time Arguments		
Deferred-delivery-time	O	8.2.1.1.1.12
Latest-delivery-time	O	8.2.1.1.1.13
Delivery Method Argument		
Requested-delivery-method	O	8.2.1.1.1.14
Physical Delivery Arguments		
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
Report Request Arguments		
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
Security Arguments		
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
Content Arguments		
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**.

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

If 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.

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

Table 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.

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

This 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.

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

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).

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

When 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.

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

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

The 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;

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

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.

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

The **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);

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

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.

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

The **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**.

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

If 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

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

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.

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

Table 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
Originator Argument		
Originator-name	M	8.2.1.1.1.1
Recipient Arguments		
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
Conversion Arguments		
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
Delivery Method Argument		
Requested-delivery-method	O	8.2.1.1.1.14

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

Table 7 – Probe-submission Arguments

Argument	Presence	Clause
Physical Delivery Argument		
Physical-rendition-attributes	O	8.2.1.1.1.20
Report Request Argument		
Originator-report-request	M	8.2.1.1.1.22
Security Arguments		
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
Content Arguments		
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.

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

Table 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.

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

Table 10 – Cancel-deferred-delivery Arguments

Argument	Presence	Clause
Submission Argument		
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
Submission Control Arguments		
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

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

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.

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

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

Table 13 – Submission-control Results

Result	Presence	Clause
"Waiting" Results		
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.

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

Table 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.

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

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.

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

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
Delivery Arguments		
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
Originator Argument		
Originator-name	M	8.2.1.1.1.1
Recipient Arguments		
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
Priority Argument		
Priority	C	8.2.1.1.1.8
Conversion Arguments		
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
Delivery Method Argument		
Requested-delivery-method	C	8.2.1.1.1.14

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

Table 15 – Message-delivery Arguments

Argument	Presence	Clause
Physical Delivery Arguments		
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
Security Arguments		
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
Content Arguments		
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.

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

The **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.

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

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

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
Proof of Delivery Results		
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

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

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
Subject Submission Argument		
Subject-submission-identifier	M	8.3.1.2.1.1
Recipient Arguments		
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
Report Envelope Arguments		
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
Conversion Arguments		
Converted-encoded-information-types	C	8.3.1.2.1.6

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

Table 18 – Report-delivery Arguments

Argument	Presence	Clause
Supplementary Information Arguments		
Supplementary-information	C	8.3.1.2.1.7
Physical-forwarding-address	C	8.3.1.2.1.8
Delivery Arguments		
Message-delivery-time	C	8.3.1.2.1.9
Type-of-MTS-user	C	8.3.1.2.1.10
Non-delivery Arguments		
Non-delivery-reason-code	C	8.3.1.2.1.11
Non-delivery-diagnostic-code	C	8.3.1.2.1.12
Security Arguments		
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
Content Arguments		
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.

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

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;

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

ms: 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;

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

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;

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

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

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;

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

unauthorised-originally-intended-recipient-name: the OR-name of the originally intended recipient of the redirected or DL-expanded message is unauthorised for security reasons;

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;

unreliable-system: delivery of the subject-message would require that the subject-message be transferred to an insecure system, which is incompatible with the message security label.

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

authentication-failure-on-subject-message: validation of the content-integrity-check, message-origin-authentication-check, or message-token (i.e. signature, or any other token data) argument of the subject-message failed, and therefore the contents of the subject-message could not be authenticated or validated;

decryption-failed: the subject-message content could not be decrypted;

decryption-key-unobtainable: the required key could not be obtained to decrypt the message-token encrypted-data or for content confidentiality;

double-envelope-creation-failure: the security policy required the creation of an outer envelope to protect the subject-message. However, the MTA was unable to create the outer envelope;

double-enveloping-message-restoring-failure: the subject-message contained an inner envelope, but failure of security services on the outer envelope prevented the MTA from extracting the inner message for subsequent processing;

failure-of-proof-of-message: a fault was detected in the proof-of security arguments in the subject-message;

integrity-failure-on-subject-message: validation of the content-integrity-check argument of the subject-message failed, and therefore the contents of the subject-message could not be validated;

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

key-failure: the required keys could not be obtained;

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

operation-security-failure: the transfer or delivery operation failed for security reasons;

repudiation-failure-of-message: the security policy required use of a signature with non-repudiation properties, but the subject-message was not signed with a non-repudiable signature on origination;

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

token-decryption-failed: the message token could not decrypted;

token-error: an error has been detected with the message-token argument of the subject-message;

unknown-security-label: the security policy identifier in the message security label is not recognised by the recipient UA or MTA. Such a policy is not supported by that system;

unsupported-algorithm-identifier: the recipient does not support the algorithm identifiers used in the security argument of the subject-message;

unsupported-security-policy: the recipient does not support the required security-policy, as identified in the message-security-label argument of subject-message.

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

8.3.1.2.1.13 Reporting-MTA-certificate

This argument contains the **certificate** of the MTA that generated the report. It shall be generated by a trusted source (e.g., a certification-authority), and may be supplied by the reporting-MTA if a **report-origin-authentication-check** is supplied.

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

The reporting-MTA's public-asymmetric-encryption-key may be used by the originator of the message, and any MTA through which the report is transferred, to validate the **report-origin-authentication-check**.

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

8.3.1.2.1.14 Report-origin-authentication-check

This argument provides the originator of the subject-message (or -probe), and any other MTA through which the report is transferred, with a means of authenticating the origin of the report (to provide the Report Origin Authentication element-of-service as defined in ITU-T Rec. X.400 | ISO/IEC 10021-1). It may be generated by the reporting-MTA if a **message-** (or **probe-**) **origin-authentication-check** was present in the subject.

The **report-origin-authentication-check** provides proof of the origin of the report (Report Origin Authentication), and proof of association between the **message-security-label** and the report.

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

The **report-origin-authentication-check** contains the **report-origin-authentication-algorithm-identifier** and an asymmetrically-encrypted hashed version of:

the **report-origin-authentication-algorithm-identifier**;

the **content-identifier** of the subject;

the **message-security-label** of the subject;

and all values of the following (per-recipient) arguments:

the **actual-recipient-name**,

the **originally-intended-recipient-name**, and:

for a delivery-report:

the **message-delivery-time**,

the **type-of-MTS-user**,

the **recipient-certificate** if requested by the originator of the message for recipients to which the report relates,

the **proof-of-delivery** if requested by the originator of the message for recipients to which the report relates and if the report is on a message; or

for a non-delivery-report:

the **non-delivery-reason-code**, and

the **non-delivery-diagnostic-code**.

Optional components are included in the **report-origin-authentication-check** if they are present in the report.

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

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

8.3.1.2.1.15 Content-type

This argument identifies the type of the **content** of the message (see 8.2.1.1.1.34). It shall be generated by the reporting-MTA. This argument may be absent on reception only if the report has been originated from or transferred through a 1984 system.

8.3.1.2.1.16 Returned-content

This argument contains the **content** of the subject-message if the originator of the subject-message indicated that the **content** was to be returned (see 8.2.1.1.1.23). It shall be generated by the originator of the message, and may be returned by the MTS (if the reporting-MTA or originating-MTA supports the Return of Content element-of-service).

This argument may only be present if there is at least one non-delivery report in the Report-delivery, and if the recipient of the report is the originator of the subject-message (and not, for example, the owner of a DL (see 8.3.1.2.1.4)).

This argument shall not be present if any **encoded-information-type** conversion has been performed on the **content** of the subject-message.

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

8.3.1.2.1.17 Reporting-MTA-name

This argument identifies the MTA which created the report. It comprises an MTA-name, a global-domain-identifier, and optionally a directory-name of an **MHS Message Transfer Agent** (see A.1.3 of ITU-T Rec. X.402 | ISO/IEC 10021-2). It may be generated by the reporting-MTA, but shall be generated by the reporting-MTA if required by the security policy in force.

NOTE 1 – Independent of any use for security purposes, this argument may be used for diagnostic purposes to indicate the MTA which generated the report.

NOTE 2 – The internal-trace-information also contains the name of the reporting-MTA. In environments where the internal-trace-information is not deleted at any point between originator and recipient, the internal-trace-information may be used as an alternative to this argument.

NOTE 3 – When used with services such as report-origin-authentication or proof-of-delivery, a typical security policy would require that this parameter is generated whenever such services are invoked.

8.3.1.2.2 Results

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

8.3.1.2.3 Abstract-errors

Table 19 lists the abstract-errors that may disrupt the Report-delivery abstract-operation, and for each abstract-error identifies the clause in which the abstract-error is defined.

Table 19 – Report-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

8.3.1.3 Delivery-control

The Delivery-control abstract-operation enables the MTS-user to temporarily limit the delivery-port abstract-operations that the MTS may invoke, and the messages that the MTS may deliver to the MTS-user via the Message-delivery abstract-operation.

The MTS shall 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, the MTS-user re-invokes the Delivery-control abstract-operation, or the MTS-user invokes the administration-port Register abstract-operation to impose constraints more severe than the specified controls.

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

8.3.1.3.1 Arguments

Table 20 lists the arguments of the Delivery-control abstract-operation, and for each argument qualifies its presence and identifies the clause in which the argument is defined.

Table 20 – Delivery-control Arguments

Argument	Presence	Clause
Delivery Control Arguments		
Restrict	O	8.3.1.3.1.1
Permissible-operations	O	8.3.1.3.1.2
Permissible-lowest-priority	O	8.3.1.3.1.3
Permissible-encoded-information-types	O	8.3.1.3.1.4
Permissible-content-types	O	8.3.1.3.1.5
Permissible-maximum-content-length	O	8.3.1.3.1.6
Permissible-security-context	O	8.3.1.3.1.7

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

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

8.3.1.3.1.1 Restrict

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

This argument may have one of the following values:

update: the other arguments update the prevailing controls;

remove: all temporary controls are to be removed (the default controls registered with the MTS by means of the administration-port Register abstract-operation shall apply); the other arguments are to be ignored.

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

8.3.1.3.1.2 Permissible-operations

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

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

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

report-delivery: the MTS may/may not invoke the Report-delivery abstract-operation.

Other delivery-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 may invoke on the MTS-user are unchanged. If there has been no previous invocation of the Delivery-control abstract-operation on the association, the default control registered with the MTS by means of the administration-port Register abstract-operation shall apply.

8.3.1.3.1.3 Permissible-lowest-priority

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

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 shall deliver to the MTS-user is unchanged. If there has been no previous invocation of the Delivery-control abstract-operation on the association, the default control registered with the MTS by means of the administration-port Register abstract-operation shall apply.

8.3.1.3.1.4 Permissible-encoded-information-types

This argument indicates the **encoded-information-types** that shall appear in messages that the MTS shall deliver to the MTS-user via the Message-delivery abstract-operation. It may be generated by the MTS-user.

The argument comprises **acceptable-encoded-information-types**, **unacceptable-encoded-information-types** and **exclusively-acceptable-encoded-information-types**, each of which identifies a list of specific **encoded-information-types**; see 8.4.1.1.1.3.1.

In the absence of this argument, the **permissible-encoded-information-types** that the MTS may deliver to the MTS-user are unchanged. If there has been no previous invocation of the Delivery-control abstract-operation on the association, the default control registered with the MTS by means of the administration-port Register abstract-operation shall apply.

8.3.1.3.1.5 Permissible-content-types

This argument indicates the only content-types that shall appear in messages that the MTS shall deliver to the MTS-user via the Message-delivery abstract-operation. It may be generated by the MTS-user.

The **permissible-content-types** specified shall be among those allowed long-term due to a previous invocation of the administration-port Register abstract-operation (**deliverable-content-types**).

In the absence of this argument, the **permissible-content-types** that the MTS may deliver to the MTS-user are unchanged. If there has been no previous invocation of the Delivery-control abstract-operation on the association, the default control registered with the MTS by means of the administration-port Register abstract-operation shall apply.

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

8.3.1.3.1.6 Permissible-maximum-content-length

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

The **permissible-maximum-content-length** shall not exceed that allowed long-term due to a previous invocation of the administration-port Register abstract-operation (**deliverable-maximum-content-length**).

In the absence of this argument, the **permissible-maximum-content-length** of a message that the MTS may deliver to the MTS-user is unchanged. If there has been no previous invocation of the Delivery-control abstract-operation on the association, the default control registered with the MTS by means of the administration-port Register abstract-operation shall apply.

8.3.1.3.1.7 Permissible-security-context

This argument temporarily limits the sensitivity of delivery-port abstract-operations (delivery-security-context) that the MTS may invoke on the MTS-user. It is a temporary restriction of the **security-context** established when the association was initiated (see 8.1.1.1.1.4). It may be generated by the MTS-user.

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 delivery-port abstract-operations is unchanged.

8.3.1.3.2 Results

Table 21 lists the results of the Delivery-control abstract-operation, and for each result qualifies its presence and identifies the clause in which the result is defined.

Table 21 – Delivery-control Results

Result	Presence	Clause
'Waiting' Results		
Waiting-operations	O	8.3.1.3.2.1
Waiting-messages	O	8.3.1.3.2.2
Waiting-encoded-information-types	O	8.3.1.3.2.3
Waiting-content-types	O	8.3.1.3.2.4

8.3.1.3.2.1 Waiting-operations

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

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

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

report-delivery: the MTS is/is not holding reports, and would invoke the Report-delivery abstract-operation on the MTS-user if it were not for the prevailing controls.

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

8.3.1.3.2.2 Waiting-messages

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

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

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

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

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

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

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

8.3.1.3.2.3 Waiting-encoded-information-types

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

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

8.3.1.3.2.4 Waiting-content-types

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

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

8.3.1.3.3 Abstract-errors

Table 22 lists the abstract-errors that may disrupt the Delivery-control abstract-operation, and for each abstract-error identifies the clause in which the abstract-error is defined.

Table 22 – Delivery-control Abstract-errors

Abstract-error	Clause
Control-violates-registration	8.3.2.2
Security-error	8.3.2.3
Operation-refused	8.3.2.5

8.3.2 Abstract-errors

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

a) Delivery-control-violated
b) Control-violates-registration
c) Security-error
d) Unsupported-critical-function
e) Operation-refused.

8.3.2.1 Delivery-control-violated

The Delivery-control-violated abstract-error reports the violation by the MTS of a control on delivery-port abstract-operations imposed by the MTS-user via the Delivery-control abstract-operation.

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

8.3.2.2 Control-violates-registration

The Control-violates-registration abstract-error reports that the MTS is unable to accept the controls that the MTS-user attempted to impose on delivery-port abstract-operations because they violate existing registration parameters.

The Control-violates-registration abstract-error has no parameters.

8.3.2.3 Security-error

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

The Security-error abstract-error has the following parameters, generated by the MTS-user:

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

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

The security-problem parameter may have one of the following values for the Message-delivery or Report-delivery 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-originally-intended-recipient-name: the OR-name of the originally intended recipient of the redirected or DL-expanded message is unauthorised for security reasons;

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.

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

authentication-failure-on-subject-message: validation of the content-integrity-check, message-origin-authentication-check, or message-token (i.e. signature, or any other token data) argument of the message failed, and therefore the contents of the message could not be authenticated or validated;

decryption-failed: the message content could not decrypted;

decryption-key-unobtainable: the required key could not be obtained to decrypt the message-token encrypted-data or for content confidentiality;

failure-of-proof-of-message: a fault was detected in the proof-of security arguments in the message;

integrity-failure-on-subject-message: validation of the content-integrity-check argument of the message failed, and therefore the contents of the message could not be validated;

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

key-failure: the required keys could not be obtained;

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

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

repudiation-failure-of-message: the security policy required use of a signature with non-repudiation properties, but the message was not signed with a non-repudiable signature on origination;

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

token-decryption-failed: the message token could not decrypted;

token-error: An error has been detected with the message-token argument of the message;

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

unsupported-algorithm-identifier: the recipient does not support the algorithm identifiers used in the security argument of the message;

unsupported-security-policy: the recipient does not support the required security-policy, as identified in the message-security-label argument of message.

The security-problem parameter may have one of the following values for the Delivery-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 Delivery-control operation failed for security reasons.

8.3.2.4 Unsupported-critical-function

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

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

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

8.3.2.5 Operation-refused

The Operation-refused abstract-error indicates that the MTS has refused to perform an operation due to local policy. The Operation-refused error has two parameters, the **refused-argument** and the **refusal-reason**, generated by the MTS.

The **refused-argument** parameter indicates which argument of the operation caused the refusal to perform. For the Delivery-control operation it shall indicate one of the arguments listed in Table 20, or one of the component arguments of deliverable-class, or an extension argument. For the Register operation it shall indicate one of the arguments listed in Table 23, or an extension argument.

The **refusal-reason** parameter shall have one of the following values:

facility-unavailable: The user has attempted to use a facility which the MTS does not make available to its users.

facility-not-subscribed: The user has attempted to use a facility which is subject to subscription, and to which the user has not subscribed.

parameter-unacceptable: The user has specified a parameter value which the MTS cannot accept.

8.4 Administration Port

This clause defines the abstract-operations and abstract-errors which occur at an administration-port.

8.4.1 Abstract-operations

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

a) Register

b) Change-credentials.

8.4.1.1 Register

The Register abstract-operation enables an MTS-user to make long-term changes to various parameters of the MTS-user held by the MTS concerned with delivery of messages to the MTS-user, and to retrieve the current settings of these parameters.

Such changes remain in effect until overridden by re-invocation of the Register abstract-operation. However, some parameters may be temporarily overridden by invocation of the Delivery-control abstract-operation.

NOTE 1 – This abstract-operation shall be invoked before any other submission-port, delivery-port or administration-port abstract-operation may be used, or an equivalent registration by local means shall have taken place.

NOTE 2 – This abstract-operation does not encompass the standing parameters implied by the Alternate Recipient Assignment element-of-service defined in ITU-T Rec. X.400 | ISO/IEC 10021-1. The manner in which those parameters are supplied and modified are a local matter.

NOTE 3 – Mechanisms other than register may be used to assign values to any of the registration parameters.

NOTE 4 – The definition of the Register abstract-operation for use in a 1988 Application Context is in Annex C.

8.4.1.1.1 Arguments

Table 23 lists the arguments of the Register abstract-operation, and for each argument qualifies its presence and identifies the clause in which the argument is defined.

Table 23 – Register Arguments

Argument	Presence	Clause
Registration Arguments		
User-name	O	8.4.1.1.1.1
User-address	O	8.4.1.1.1.2
Deliverable-classes	O	8.4.1.1.1.3
Recipient-assigned-redirections	O	8.4.1.1.1.4
Restricted-delivery	O	8.4.1.1.1.5
Retrieve-registrations	O	8.4.1.1.1.6

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

Table 23 – Register Arguments

Argument	Presence	Clause
Default Delivery Control Arguments		8.4.1.1.1.7
Permissible-operations	O	8.3.1.3.1.2
Permissible-lowest-priority	O	8.3.1.3.1.3
Permissible-encoded-information-types	O	8.3.1.3.1.4
Permissible-content-types	O	8.3.1.3.1.5
Permissible-maximum-content-length	O	8.3.1.3.1.6

8.4.1.1.1.1 User-name

This argument contains the **OR-name** of the MTS-user, if the **user-name** is to be changed. It may be generated by the MTS-user.

An MD is not required to provide MTS-users with the ability to change their own **OR-name**. If it does so, the MD may restrict that ability. It may prohibit certain MTS-users from changing their **OR-names**, or it may restrict the scope of the change to a locally defined subset of the components of their **OR-names**. A proposed new **OR-name** shall be rejected if its OR-address is already assigned to another MTS-user or a DL.

In the absence of this argument, the **user-name** of the MTS-user remains unchanged.

8.4.1.1.1.2 User-address

This argument contains the **user-address** of the MTS-user, if it is required by the MTS and if it is to be changed. It may be generated by the MTS-user.

The **user-address** may contain one of the following forms of address of the MTS-user:

the **X.121-address** and/or the **TSAP-ID** (transport service access point identifier); or

the **PSAP-address** (presentation service access point address).

Other forms of **user-address** may be defined in addenda or future versions of this Recommendation | International Standard.

In the absence of this argument, the **user-address** of the MTS-user (if any) remains unchanged.

8.4.1.1.1.3 Deliverable-classes

This argument contains all the sets of criteria that determine which messages shall be delivered to the MTS-user, if any of these criteria are to be changed. If present, this argument replaces the previously registered **deliverable-classes**. It may be generated by the MTS-user.

Each set of criteria forms a **deliverable-class**. The **deliverable-class** optionally contains **encoded-information-types-constraints**, **deliverable-content-types**, **deliverable-maximum-content-length**, and **deliverable-security-labels**. The absence of values for a particular component indicates that no restriction on values of that component exists in this **deliverable-class**.

The MTS shall deliver a message to the MTS-user only if the message meets all the criteria in at least one **deliverable-class** in the registered set.

In the absence of this argument, the **deliverable-classes** shall remain unchanged.

8.4.1.1.1.3.1 Encoded-information-types-constraints

This component indicates the **encoded-information-types** that the MTS shall permit to appear in messages delivered to the MTS-user, if they are to be constrained within a **deliverable-class**.

The component comprises **acceptable-encoded-information-types**, **unacceptable-encoded-information-types**, and **exclusively-acceptable-encoded-information-types**, each of which identifies a list of specific **encoded-information-types**.

If a message has no **encoded-information-types** it will always satisfy any **encoded-information-types-constraints**.

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

If the **encoded-information-types** of the message to be delivered are incompatible with the **encoded-information-types-constraints**, then the message does not satisfy the constraints of this **deliverable-class**, and no other criteria of the **deliverable-class** need be considered.

The MTS determines whether a message satisfies the **encoded-information-types-constraints** of a **deliverable-class** according to the procedure defined in 14.3.4.4, item 7 (c).

The **encoded-information-types** in a message to be delivered are regarded as those which would be present in the message after all conversions (if any) have been performed.

Depending on local requirements or the capabilities provided by a user's computing environment, a user may choose one of the following registrations which:

a) allows delivery of all messages independent of the **encoded-information-types** they contain. In this case no **encoded-information-types-constraints** need be registered.

b) allows delivery of all messages except those which contain at least one **encoded-information-type** in the set of registered **unacceptable-encoded-information-types**. In this case no **acceptable-encoded-information-types** or **exclusively-acceptable-encoded-information-types** need be registered.

NOTE 1 – For example, this registration may for example be appropriate for an MS-user that does not support the Voice body part, in order to prevent messages containing large Voice body parts from consuming the storage space available for delivered messages.

c) allows delivery of the message if it contains at least one of the registered **acceptable-encoded-information-types**. In this case no **unacceptable-encoded-information-types** or **exclusively-acceptable-encoded-information-types** need be registered.

NOTE 2 – For example, an IPMS-user may require that all messages containing an IA5 Text body part are delivered. After reading the IA5 Text body parts, the user may be able to evaluate the importance of the information contained in the other body parts, and decide whether to seek other means to process these body parts.

d) requires all **encoded-information-types** in the message to be registered as **exclusively-acceptable-encoded-information-types**, and rejects as undeliverable otherwise. In this case **acceptable-encoded-information-types** or **unacceptable-encoded-information-types** need be registered.

Note 3 – This may be appropriate if the user's UA supports a relatively small set of encoded-information-types. This is identical to the service supported by the Register-88 abstract-operation.

e) allows delivery of the message if it does not contain any the registered **unacceptable-encoded-information-types**, and either contains at least one **encoded-information-type** registered in **acceptable-encoded-information-types**, or only contains **encoded-information-types** registered as **exclusively-acceptable-encoded-information-types**. In this case, **unacceptable-encoded-information-types**, **acceptable-encoded-information-types**, and **exclusively-acceptable-encoded-information-types** may all be registered.

NOTE 4 – This satisfies the requirements in b), c), and d). For example, an IPMS-user may use this combination to ensure that Voice body parts are never delivered, File Transfer body parts are always delivered (subject to the absence of Voice body parts), and where neither of these body part types is present, only those messages containing a prescribed set of body parts are delivered.

The MTS will return an error if the MTS-user attempts to register an **encoded-information-type** both in **unacceptable-encoded-information-types** and in either of **acceptable-encoded-information-types** or **exclusively-acceptable-encoded-information-types**.

The **acceptable-encoded-information-types** and **exclusively-acceptable-encoded-information-types** also indicate the possible **encoded-information-types** which implicit conversion may usefully produce.

In the absence of this component, the **encoded-information-types-constraints** shall be unconstrained.

8.4.1.1.1.3.2 Deliverable-content-types

This component indicates the **content-types** that the MTS shall permit to appear in messages delivered to the MTS-user, if they are to be constrained within a **deliverable-class**.

If the **content-length** of the message to be delivered exceeds that specified by the **deliverable-maximum-content-length**, then the message does not satisfy the constraints of this **deliverable-class** and no other criteria of the **deliverable-class** need be considered. The MTS-user may register to receive the **unidentified content-type**.

In the absence of this component, the **deliverable-content-types** shall be unconstrained.

8.4.1.1.1.3.3 Deliverable-maximum-content-length

This component contains the **content-length**, in octets, of the longest-content message that the MTS shall permit to appear in messages delivered to the MTS-user, if it is to be constrained within a **deliverable-class**.

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

If the **content-length** of the message to be delivered exceeds that specified by the **deliverable-maximum-content-length**, then the message does not satisfy the constraints of this **deliverable-class** and no other criteria of the **deliverable-class** need be considered.

In the absence of this component, the **deliverable-maximum-content-length** of messages shall be unconstrained.

8.4.1.1.1.3.4 Deliverable-security-labels

This component contains the **security-labels** of the MTS-user, if they are to be constrained within a **deliverable-class**.

If the **security-labels** of the message to be delivered do not match those specified by the **deliverable-security-labels**, then the message does not satisfy the constraints of this **deliverable-class** and no other criteria of the **deliverable-class** need be considered.

Some security-policies may only permit the **deliverable-security-labels** to be changed in this way if a secure link is employed. Other local means of changing the **deliverable-security-labels** in a secure manner may be provided.

In the absence of this component, the **deliverable-security-labels** shall be unconstrained.

8.4.1.1.1.4 Recipient-assigned-redirections

This argument contains, if the assignment of alternate-recipients is to be changed, an ordered list of the **OR-names** of **recipient-assigned-alternate-recipient**s and, optionally, one or more **redirection-classes** associated with each alternate-recipient. If this argument is present its value completely replaces any previous assignment of alternate-recipients. It may be generated by the MTS-user.

If one or more **recipient-assigned-alternate-recipients** is specified then each message (or report) for the MTS-user shall be redirected to the first alternate-recipient for which the message (or report) meets the criteria in one of the **redirection-classes** associated with that alternate-recipient. Those messages (or reports) meeting the criteria of none of the **redirection-classes** for any **recipient-assigned-alternate-recipient** shall continue to be delivered to the MTS-user. The order of alternate-recipients is specified by the MTS-user. The absence of any **redirection-classes** indicates an alternate-recipient to which all messages (and reports), except those meeting more specific **redirection-classes** associated with preceding alternate-recipients, shall be redirected. The absence of the **recipient-assigned-alternate-recipient** indicates delivery to the MTS-user.

NOTE – If present in the **recipient-assigned-redirections** list, the absent **redirection-class** should be last in the list as no later elements will ever be used.

The **redirection-class** optionally contains a maximum **content-length** and optionally sets of values for each of: **encoded-information-types**, **content-type**, **deliverable-security-labels**, **restriction**, and **priority**. The absence of values for a particular type indicates that no restriction on values of that type exists in this **redirection-class**. The **redirection-class** also indicates the types of MHS information object to which the **redirection-class** applies: messages only, reports only, or both messages and reports.

The **recipient-assigned-alternate-recipient** shall contain the **OR-name** of the alternate-recipient.

If the **recipient-assigned-redirections** argument contains a single element with both the **recipient-assigned-alternate-recipient** and the **redirection-class** absent then no **recipient-assigned-redirections** is registered.

When **recipient-assigned-redirections** and **deliverable-classes** are both registered, redirection takes precedence over delivery restrictions.

In the absence of this argument, the **recipient-assigned-redirections**, if any, remain unchanged.

8.4.1.1.1.5 Restricted-delivery

This argument indicates the **OR-names** of other MTS-users from whom the MTS-user is willing (or unwilling) to receive messages, if **restricted-delivery** is to be changed. It comprises an ordered list of **restrictions**. If the **restricted-delivery** argument is present its value completely replaces any previous registered value. It may be generated by the MTS-user.

The MTS shall reject as undeliverable any message for the MTS-user which originates from, or is redirected by, or is dl-expanded by another MTS-user from which the MTS-user does not consent to accept delivery. Each restriction may specify a source which is permitted or which is disallowed, either as a complete **OR-name** or as an **OR-name** pattern.

If one or more **restriction** is registered then the sources (**originator-name**, **redirection-history**, **DL-expansion-history**) of each message are compared to the ordered list of **restrictions** until a match occurs. The comparison stops immediately a match with a **restriction** occurs, and the message is delivered if permitted or rejected as undeliverable if not permitted. If there is no matching **restriction** the message is delivered.

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

Procedures for determining exact and pattern matches of **OR-names** are specified in ITU-T Rec. X.402 | ISO/IEC 10021-2.

The MTS-user may register to receive all messages, which is the state before any **restricted-delivery** registration, by specifying a single **restriction** in which all source-types are permitted and the source-name omitted.

Where **restricted-delivery** and **recipient-assigned-redirections** are both registered, redirection takes precedence over **restricted-delivery**.

In the absence of this argument, **restricted-delivery** shall remain unchanged.

8.4.1.1.1.6 Retrieve-registrations

This argument indicates the individual registrations that the MTS-user requests to be returned in the result of the Register abstract-operation. It may be generated by the MTS-user.

The result returned reflects the state of registered information after all other arguments of Register have been processed.

This argument contains an element corresponding to each of the other arguments of Register, each of which, if set, requests the registered value of the corresponding argument.

In the absence of this argument, no registration information is requested.

8.4.1.1.1.7 Default-delivery-control-arguments

The default control arguments are the same as the arguments of the Delivery-control abstract-operation, and are defined in 8.3.1.3.1. Except for **restrict** and **permissible-security-context**, they may be generated by the MTS-user.

The default controls are registered as arguments of the Register abstract-operation. These defaults come into effect at the beginning of an association, and remain in effect until they are overridden by an invocation of the Delivery-control abstract-operation.

The default control arguments shall not admit messages whose delivery are prohibited by the prevailing registered values of the **encoded-information-types-constraints** argument, the **deliverable-content-types** argument or the **deliverable-maximum-content-length** argument.

8.4.1.1.2 Results

The Register abstract-operation returns an empty result unless an extension result is present, or the **retrieve-registrations** argument was present in the invocation. In the latter case, those registrations identified in the **retrieve-registrations** argument are returned.

The results are identical to the arguments of the Register abstract-operation listed in Table 23 except that **retrieve-registrations** is absent.

8.4.1.1.3 Abstract-errors

Table 24 lists the abstract-errors that may disrupt the Register abstract-operation, and for each abstract-error identifies the clause in which the abstract-error is defined.

Table 24 – Register Abstract-errors

Abstract-error	Clause
Register-rejected	8.4.2.1
Remote-bind-error	8.2.2.10
Operation-refused	8.3.2.5
Security-error	8.4.2.4

8.4.1.2 Change-credentials

The Change-credentials abstract-operation enables the MTS-user to change the MTS-user's simple-authentication **credentials** held by the MTS, or enables the MTS to change the MTS's simple-authentication **credentials** held by the MTS-user.

The **credentials** are exchanged during the establishment of an association for the mutual authentication of identity of the MTS-user and the MTS.

The successful completion of the abstract-operation signifies that the **credentials** have been changed.

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

The disruption of the abstract-operation by an abstract-error indicates that the **credentials** have not been changed, either because the old **credentials** were incorrectly specified or that the new **credentials** are unacceptable.

8.4.1.2.1 Arguments

Table 25 lists the arguments of the Change-credentials abstract-operation, and for each argument qualifies its presence and identifies the clause in which the argument is defined.

Table 25 – Change-credentials Arguments

Argument	Presence	Clause
Credential Arguments		
Old-credentials	M	8.4.1.2.1.1
New-credentials	M	8.4.1.2.1.2

8.4.1.2.1.1 Old-credentials

This argument contains the current (old) **credentials** of the invoker of the abstract-operation, held by the performer of the abstract-operation. It shall be generated by the invoker of the abstract-operation.

If only simple-authentication is used, the **credentials** comprise a simple **password** associated with the **user-name**, or **MTA-name**, of the invoker.

8.4.1.2.1.2 New-credentials

This argument contains the proposed new **credentials** of the invoker of the abstract-operation, to be held by the performer of the abstract-operation. It shall be generated by the invoker of the abstract-operation.

The security policy in force may restrict the type of **new-credentials**.

8.4.1.2.2 Results

The Change-credentials abstract-operation returns an empty result as indication of success.

8.4.1.2.3 Abstract-errors

Table 26 lists the abstract-errors that may disrupt the Change-credentials abstract-operation, and for each abstract-error identifies the clause in which the abstract-error is defined.

Table 26 – Change-credentials Abstract-errors

Abstract-error	Clause
New-credentials-unacceptable	8.4.2.2
Old-credentials-incorrectly-specified	8.4.2.3
Remote-bind-error	8.2.2.10
Security-error	8.4.2.4

8.4.2 Abstract-errors

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

a) Register-rejected
b) New-credentials-unacceptable
c) Old-credentials-incorrectly-specified
d) Security-error.

8.4.2.1 Register-rejected

The Register-rejected abstract-error reports that the requested parameters cannot be registered because one or more are improperly specified.

The Register-rejected abstract-error has no parameters.

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

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

8.4.2.2 New-credentials-unacceptable

The New-credentials-unacceptable abstract-error reports that the **credentials** cannot be changed because the **new-credentials** are unacceptable.

The New-credentials-unacceptable abstract-error has no parameters.

8.4.2.3 Old-credentials-incorrectly-specified

The Old-credentials-incorrectly-specified abstract-error reports that the **credentials** cannot be changed because the current (**old-**) **credentials** were incorrectly specified.

The Old-credentials-incorrectly-specified abstract-error has no parameters.

8.4.2.4 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 security-problem parameter may have one of the following values for the Register abstract-operation:

forbidden-user-security-label-register: the user is not permitted to use the Register operation to change security labels;

invalid-security-label-update: the proposed value of deliverable-security-label is not acceptable to the security-policy;

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

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

redirection-prohibited: the security-policy prohibits registration of recipient-assigned-redirections;

refused-alternate-recipient-name: the requested alternate 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-security-label-update: the user is not allowed by the security-policy to update the deliverable-security-label ;

unauthorised-user-name: the proposed new value of user-name is unacceptable, for security reasons.

The security-problem parameter may have one of the following values for the Change-credentials operation:

operation-security-failure: the Change-credentials operation failed for security reasons;

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

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

8.5 Common Parameter Types

This clause defines a number of common parameter types of the MTS Abstract Service.

8.5.1 MTS-identifier

MTS-identifiers are assigned by the MTS to distinguish between messages and probes at the MTS Abstract Service, and between messages, probes and reports within the MTS.

The **MTS-identifier** assigned to a message at a submission-port (**message-submission-identifier**) is identical to the corresponding **message-identifier** at a transfer-port and corresponding **message-delivery-identifier** at a delivery-port. Similarly, the **MTS-identifier** assigned to a probe at a submission-port (**probe-submission-identifier**) is identical to the corresponding **probe-identifier** at a transfer-port. **MTS-identifiers** are also assigned to reports at transfer-ports (**report-identifier**).

An **MTS-identifier** comprises:

a **local-identifier** assigned by the MTA, which unambiguously identifies the related event within the MD;

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

the **global-domain-identifier** of the MD, which ensures that the **MTS-identifier** is unambiguous throughout the MTS.

8.5.2 Global-domain-identifier

A **global-domain-identifier** unambiguously identifies an MD within the MHS.

A **global-domain-identifier** is used to ensure that an **MTS-identifier** is unambiguous throughout the MTS, and for identifying the source of a **trace-information-element**.

In the case of an ADMD, a **global-domain-identifier** consists of the **country-name** and the **administration-domain-name** of the MD.

In the case of a PRMD, a **global-domain-identifier** consists of the **country-name** and, optionally, the **administration-domain-name** of the associated ADMD, plus a **private-domain-identifier**. The **private-domain-identifier** is a unique identification of the PRMD, and may be identical to the PRMD's **private-domain-name**. As a national matter, this identification may be either relative to the country denoted by the **country-name** or relative to the associated ADMD. If the identification is relative to the associated ADMD then that **administration-domain-name** shall be present. Where the **administration-domain-name** is optional in the Abstract Service but mandatory in the abstract syntax, and no value is specified, it shall be encoded as a single space (see 18.3.1 in ITU-T Rec. X.402 | ISO/IEC 10021-2).

NOTE – The distinction between **private-domain-identifier** and **private-domain-name** has been retained for backward compatibility with CCITT Recommendation X.411 (1984). Often they will be identical.

8.5.3 MTA-name

An **MTA-name** is an identifier for an MTA that uniquely identifies the MTA within the MD to which it belongs.

8.5.4 Time

A **Time** parameter is specified in terms of UTC (Coordinated Universal Time), and may optionally also contain an offset to UTC to convey the local time. The precision of the time of day is to either one second or one minute, determined by the generator of the parameter.

8.5.5 OR-name

An **OR-name** identifies the originator or recipient of a message according to the principles of naming and addressing described in ITU-T Rec. X.402 | ISO/IEC 10021-2.

At a submission-port, an **OR-name** comprises an **OR-address**, or a **directory-name**, or both (**OR-address-and-or-directory-name**). At all other types of port, an **OR-name** comprises an **OR-address** and, optionally, a **directory-name** (**OR-address-and-optional-directory-name**). A **directory-name** and an **OR-address** may each denote an individual originator or recipient, or a DL.

A **directory-name** is as defined in ITU-T Rec. X.501 | ISO/IEC 9594-2. The MTS uses the **directory-name** only when the **OR-address** is absent or invalid.

An **OR-address** comprises a number of **standard-attributes** selected from those defined in ITU-T Rec. X.402 | ISO/IEC 10021-2, and optionally a number of attributes defined by the MD to which the originator/recipient subscribes (**domain-defined-attributes**).

In the abstract syntax definition in clause 9, the standard attributes are represented by **built-in-standard-attributes** and by **extension-standard-attributes** and the domain-defined attributes are represented by **built-in-domain-defined-attributes** and by **extension-domain-defined-attributes**.

Clause 18.5 of ITU-T Rec. X.402 | ISO/IEC 10021-2 specifies several **OR-address** forms. These define which standard and domain-defined attributes may be used together to construct a valid **OR-address**.

Clause 18.3 of ITU-T Rec. X.402 | ISO/IEC 10021-2 specifies rules indicating the character sets – numeric, printable, and teletex – from which the values of a particular standard attribute may be drawn, and it also defines the valid combinations of the different variants of that standard attribute in the abstract syntax.

8.5.6 Encoded-information-types

The **encoded-information-types** of a message are the kind(s) of information that appear in its **content**. Both basic **encoded-information-types** and externally-defined **encoded-information-types** may be specified, otherwise the **encoded-information-types** of a message are **unspecified**.

The basic **encoded-information-types** are those originally defined in the CCITT Recommendation X.411 (1984). The **unknown** type is used to indicate an **encoded-information-type** which is not in this instance indicated by an externally-defined **encoded-information-type**, and is other than the following types. The **ia5-text** (teleprinter) type is

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

defined in CCITT Recommendation T.50. The **g3-facsimile** type is defined in CCITT Recommendations T.4 and T.30. The **g4-class-1** type is defined in CCITT Recommendations T.5, T.6, T.400 and T.503. The **teletex** type is defined in CCITT Recommendations F.200, T.61 and T.60. The **videotex** type is defined in CCITT Recommendations T.100 and T.101. The **simple-formattable-document** (**sfd**) type and the **telex** type were defined in CCITT Recommendation X.420 (1984) (SFD and TLX body parts are no longer defined in any CCITT Recommendation). The **mixed-mode** type is defined in CCITT Recommendations T.400 and T.501.

NOTE – The **unknown** encoded information type is provided to represent externally-defined **encoded-information-types** when downgrading for 1984 systems (and remains present after a subsequent upgrade), and also for use in cases where no externally-defined **encoded-information-type** has been defined for a particular type of information.

Externally-defined **encoded-information-types** are those which are not basic **encoded-information-types**.

In the abstract syntax definition in clause 9, the **encoded-information-types** are the logical union of **built-in-encoded-information-types** and **extended-encoded-information-types**. The latter are those to which object-identifiers have been allocated by an appropriate authority. They include both standardised and privately-defined **encoded-information-types**.

A basic **encoded-information-type** may be represented equivalently by a bit in the **built-in-encoded-information-types** or by an **extended-encoded-information-type**. Annex A acts as the registration authority for the object-identifiers to be used as the **extended-encoded-information-type** registrations of the basic **encoded-information-types**.

An externally-defined **encoded-information-type** is always represented by an **extended-encoded-information-type**. Other standards define object-identifiers that may be used as **extended-encoded-information-types**.

Non-basic-parameters are defined for the **g3-facsimile** and **teletex** basic **encoded-information-types** for backwards compatibility with the CCITT Recommendation X.411 (1984) only. It is recommended that for each required combination of a basic **encoded-information-type** and a specific set of **non-basic-parameters**, an externally-defined **encoded-information-type** be defined and used in preference.

NOTE – **non-basic-parameters** are likely to be removed from a future version of this Recommendation | International Standard.

The **non-basic-parameters** for **g3-facsimile** correspond to the three- or four-octet Facsimile Information Field (FIF) conveyed by the Digital Command Signal (DCS) defined in CCITT Recommendation T.30. The parameters are: **two-dimensional**, **fine-resolution**, **unlimited-length**, **b4-length**, **a3-width**, **b4-width** and **uncompressed**.

The **non-basic-parameters** for **teletex** correspond to the non-basic terminal capability conveyed by the Command Document Start (CDS) defined in CCITT Recommendation T.62. The parameters are: optional **graphic-character-sets**, optional **control-character-sets**, optional **page-formats**, optional **miscellaneous-terminal-capabilities**, and a **private-use** parameter.

Where **non-basic-parameters** are indicated, these parameters represent the logical 'OR' of the **non-basic-parameters** of each instance on the **encoded-information-type** in a message **content**. Thus, this parameter only serves to indicate whether there is **encoded-information-type** compatibility, or whether conversion is required. If conversion is required, the message **content** shall be inspected to determine which **non-basic-parameters** apply to any instance of the **encoded-information-type**.

8.5.7 Certificate

A **certificate** may be used to convey a verified copy of the public-asymmetric-encryption-key of the subject of the **certificate**.

A **certificate** contains one or more items of certification information. Each instance of certification information contains the following parameters:

signature-algorithm-identifier: an **algorithm-identifier** for the algorithm used by the certification-authority that issued the **certificate** to compute the **signature**;

issuer: the **directory-name** of the certification-authority that issued the **certificate**;

validity: a date and time of day before which the **certificate** should not be used, and a date and time of day after which the **certificate** should not be relied upon;

subject: the **directory-name** of the subject of the **certificate**;

subject-public-key: the public-asymmetric-encryption-keys of the subject;

algorithm: the **algorithm-identifiers**, associated with a **subject-public-key**;

signature: an asymmetrically encrypted, hashed version of the above parameters computed by the certification-authority that issued the **certificate** using the algorithm identified by the **signature-algorithm-identifier** and the certification-authority's secret-asymmetric-encryption-key.

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

Version 3 certificates shall be used when the originator or recipients have more than one set of public information to be certified.

Version 3 certificates support an extension capability to the information that is to be signed as part of the certificate. The standard certificate extensions are defined by ITU-T Rec. X.509 | ISO/IEC 9594-8. The various standard extensions can be used to indicate the purpose of the information contained in the certificate. The standard extensions are summarised as:

- **Key and policy information**: These certificate and CRL extensions convey additional information about the keys involved, including key identifiers for subject and issuer keys, indicators of intended or restricted key usage, and indicators of certificate policy.
- **Subject and issuer attributes**: These certificate and CRL extensions support alternative names, of various name forms, for a certificate subject, a certificate issuer, or a CRL issuer. These extensions can also convey additional attribute information about the certificate subject, to assist a certificate user in being confident that the certificate subject is a particular person or entity.
- **Certification path constraints**: These certificate extensions allow constraint specifications to be included in CA-certificates, i.e. certificates for CAs issued by other CAs, to facilitate the automated processing of certification paths when multiple certificate policies are involved. Multiple certificate policies arise when policies vary for different applications in an environment or when interoperation with external environments occurs. The constraints may restrict the types of certificates that can be issued by the subject CA or that may occur subsequently in a certification path.
- **Basic CRL extensions**: These CRL extensions allow a CRL to include indications of revocation reason, to provide for temporary suspension of a certificate, and to include CRL-issue sequence numbers to allow certificate users to detect missing CRLs in a sequence from one CRL issuer.
- **CRL distribution points and delta-CRLs**: These certificate and CRL extensions allow the complete set of revocation information from one CA to be partitioned into separate CRLs and allow revocation information from multiple CAs to be combined in one CRL. These extensions also support the use of partial CRLs indicating only changes since an earlier CRL issue.

The **key and policy information extensions** may be used to indicate which certificate is associated with which digital signature accompanying the message, including the **message-origin-authentication-check**, and individual recipient's **content-integrity-check** and **message-token**.

If the originator and a recipient of a **certificate** are served by the same certification-authority, the recipient may use the certification-authority's public-asymmetric-encryption-key to validate the **certificate**, and derive the originator's public-asymmetric-encryption-key (**subject-public-key**).

If the originator and a recipient of a **certificate** are served by different certification-authorities, the recipient may require a return-certification-path to authenticate the originator's **certificate**. The **certificate** may therefore include an associated **certification-path**.

The **certification-path** may comprise a **forward-certification-path** which includes the certificate of the certification-authority that issued the **certificate**, together with the certificates of all of its superior certification-authorities. The **forward-certification-path** may also include the certificates of other certification-authorities, cross-certified by either the certification-authority that issued the **certificate**, or any of its superior certification-authorities.

A recipient of the **certificate** may complete the required return-certification-path between the recipient and the originator of the **certificate** by appending the recipient's own reverse-certification-path to the **forward-certification-path** supplied by the originator, at a common-point-of-trust. The reverse-certification-path includes the reverse-certificate of the certification-authority of the recipient of the **certificate**, together with the reverse-certificates of all of its superior certification-authorities. The reverse-certification-path may also include the reverse-certificates of other certification-authorities, cross-certified by the certification-authority of the recipient of the **certificate**, or any of its superior certification authorities.

The return-certification-path thus formed allows the recipient of the **certificate** to validate each certificate in the return-certification-path in turn, to derive the public-asymmetric-encryption-key of the certification-authority that issued the **certificate**. The recipient may then use the public-asymmetric-encryption-key of the certification-authority that issued the **certificate** to validate the **certificate**, and derive the originator's public-asymmetric-encryption-key (**subject-public-key**).

The **certification path constraints** extensions allow constraint specifications to be included in CA-certificates and thus can be used to indicate any restrictions or controls on the use of **certification-path**.

The form of a **certificate** is defined in ITU-T Rec. X.509 | ISO/IEC 9594-8 as the data-type **certificates**.

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

NOTE – The term **certificate** used in this specification differs from the use of the same term in ITU-T Rec. X.509 | ISO/IEC 9594-8. The former may optionally contain a certification path whereas the latter does not. The equivalent term in ITU-T Rec. X.509 | ISO/IEC 9594-8 to **certificate** in this specification is **certificates** with the "s".

When a **certificate** 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.

When a **certificate** is needed to validate a specific digital signature in the **content-integrity-check** or **message-token**, Version 3 certificates shall always be used. The certificate extension called **certification policies field** of the originator certificate shall indicate that the certificate (and certification-path) is to be used to by the recipient of the message to validate the specific digital signature contained in the **content-integrity-check**, or the **message-token** argument (see 8.2.1.1.1.28). If all signatures employ the same algorithm and public key, it will only be necessary to identify one policy within the **certification policies field**; otherwise, separated object identifiers will be needed for each signature type.

8.5.8 Token

A **token** may be used to convey to the recipient of the **token** protected security-relevant information. The **token** provides authentication of public security-relevant information, and confidentiality and authentication of secret security-relevant information.

The type of a **token** is identified by a **token-type-identifier**. One type of **token** is currently defined by this Service Definition: an **asymmetric-token**. Other types of **token** may be defined by addenda or future versions of this Recommendation | International Standard; for example, **tokens** based on symmetric-encryption techniques.

An **asymmetric-token** contains the following parameters:

signature-algorithm-identifier: an **algorithm-identifier** for the algorithm used by the originator of the **token** to compute the **signature**;

recipient-name: either the **OR-address-and-or-directory-name** of the intended-recipient of the **token**; or, for strong authentication in an MTA-bind, the **MTA-name** and optionally the **global-domain-identifier** of the peer MTA (i.e. the recipient of the bind-token); or, for strong authentication in an MTS-bind, the **MTA-name** and optionally the **global-domain-identifier** of the MTA where the token is generated by the MTS-user, or the **OR-address-and-optional-directory-name** of the MTS-user where the token is generated by the MTS; or, for strong authentication in an MS-bind, the **OR-address-and-optional-directory-name** of the MS-user (whether the token is generated by the MS or by the MS-user);

time: the date and time of day when the **token** was generated;

signed-data: public security-relevant information;

encryption-algorithm-identifier: an **algorithm-identifier** for the algorithm used by the originator of the **token** to compute the **encrypted-data**;

encrypted-data: secret security-relevant information encrypted by the originator of the **token** using the algorithm identified by the **encryption-algorithm-identifier** and the public-asymmetric-encryption-key of the intended-recipient of the **token**;

signature: an asymmetrically encrypted, hashed version of the above parameters computed by the originator of the **token** using the algorithm identified by the **signature-algorithm-identifier** and the originator's secret-asymmetric-encryption-key.

The form of a **token** is further defined in ITU-T Rec. X.509 | ISO/IEC 9594-8.

Symmetric algorithms may be used within the **asymmetric-token** definition provided that:

the algorithm (in either the **signature-algorithm-identifier** or the **encryption-algorithm-identifier**) is used to identify a registered symmetric cryptographic algorithm;

the management of symmetric keys (e.g., key distribution) is performed externally to the MTS.

NOTE 1 – When symmetric algorithms are used for **signed-data**, the message origin authentication check, as defined in ITU-T Rec. X.402 | ISO/IEC 10021-2, is not provided by the token. The token only provides proof that the message was signed by a holder of the symmetric key (i.e., a member of a closed user group).

NOTE 2 – The **signature-algorithm-identifier** and the **encryption-algorithm-identifier** can be individually defined and, therefore, a mixture of symmetric and asymmetric algorithms can be used with the token.

8.5.9 Security-label

Security-labels may be used to associate security-relevant information with objects within the MTS.

Security-labels may be assigned to an object in line with the security-policy in force for that object. The security-policy may also define how **security-labels** are to be used to enforce that security-policy.

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

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

Within the scope of this Service Definition, **security-labels** may be associated with messages, probes and reports (see 8.2.1.1.1.30), MTS-users (see 8.4.1.1.1.3.4), MDs, MTAs and associations between an MTS-user and an MD (or MTA) (see 8.1.1.1.1.4), or between MDs (or MTAs) (see 12.1.1.1.1.3). Beyond the scope of this Service Definition, a security-policy may, as a local matter or by bilateral agreement, additionally assign **security-labels** to other objects within the MTS (e.g., secure routes).

A **security-label** comprises a set of **security-attributes**. The **security-attributes** may include a **security-policy-identifier**, a **security-classification**, a **privacy-mark**, and a set of **security-categories**.

A **security-policy-identifier** may be used to identify the security-policy in force to which the **security-label** relates.

If present, a **security-classification** may have one of a hierarchical list of values. The basic **security-classification** hierarchy is defined in this Service Definition, but the use of these values is defined by the security-policy in force. Additional values of **security-classification**, and their position in the hierarchy, may also be defined by a security-policy as a local matter or by bilateral agreement. The basic **security-classification** hierarchy is, in ascending order: **unmarked**, **unclassified**, **restricted**, **confidential, secret**, **top-secret**.

If present, a **privacy-mark** is a printable string. The content of the printable string may be defined by a security-policy, which may define a list of values to be used, or allow the value to be determined by the originator of the **security-label**. Examples of privacy-marks include: '**IN CONFIDENCE**' and '**IN STRICTEST CONFIDENCE**'.

If present, the set of **security-categories** provide further restrictions within the context of a **security-classification** and/or **privacy-mark**, typically on a 'need-to-know' basis. The **security-categories** and their values may be defined by a security-policy as a local matter or by bilateral agreement. Examples of possible **security-categories** include caveats to the **security-classification** and/or **privacy-mark** (e.g., '**PERSONAL – **', '**STAFF – **', '**COMMERCIAL – **', etc), closed-user-groups, codewords, etc.

8.5.10 Algorithm-identifier

An **algorithm-identifier** identifies an **algorithm** and any **algorithm-parameters** required by the **algorithm**. It shall also define the ASN.1 encoding rules used.

An **algorithm-identifier** may be drawn from an international register of algorithms, or defined by bilateral agreement.

8.5.11 Password

A password comprises either an IA5 String or an Octet String.

Where the octets of an Octet String value are the encoding in an 8-bit environment of the characters of an IA5 String value, the choice between the IA5 String and the Octet String representations shall be considered insignificant.

NOTE 1 – This equivalence rule does not prohibit a password from being an Octet String value which is not the encoding of any IA5 String value.

NOTE 2 – "Encoding in an 8-bit environment" means that the most significant bit in each octet is zero and not a parity bit; this is the encoding of IA5 String characters used by ASN.1 Basic Encoding Rules. An IA5 String password should have the top bit of each octet set to zero before writing it as the value of a User Password attribute, which is defined by the Directory ITU-T Rec. X.520 | ISO/IEC 9594-6 to be an Octet String. The equivalence rule is designed to facilitate the use of this Directory attribute.

NOTE 3 – Where ASN.1 Basic Encoding Rules are used, two passwords can be compared as follows. The octets of each password value are extracted from its BER encoding (which may be primitive or constructed); the extraction technique is the same for both IA5 String and Octet String. If the extracted values are equal octet by octet, then the two passwords match.

9 Message Transfer System Abstract Syntax Definition

The abstract-syntax of the MTS Abstract Service is defined in Figure 2. Those aspects of the 1988 version of the MTS Abstract Service which differ from the 1994 version are defined in Annex C.

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

The abstract-syntax definition of the MTS Abstract Service has the following major parts:

Prologue: declarations of the exports from, and imports to, the MTS Abstract Service module (Figure 2 Parts 1 to 2).

Objects and Ports: definitions of the MTS and MTS-user objects, and their submission-, delivery- and administration-ports (Figure 2 Part 2 to 3).

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

MTS-bind and MTS-unbind: definitions of the MTS-bind and MTS-unbind used to establish and release associations between an MTS-user and the MTS (Figure 2 Parts 3 to 4).

Submission Port: definitions of the submission-port abstract-operations: Message-submission, Probe-submission, Cancel-deferred-delivery and Submission-control; and their abstract-errors (Figure 2 Parts 4 to 7).

Delivery Port: definitions of the delivery-port abstract-operations: Message-delivery, Report-delivery and Delivery-control; and their abstract-errors (Figure 2 Parts 7 to 9).

Administration Port: definitions of the administration-port abstract-operations: Register and Change-credentials; and their abstract-errors (Figure 2 Parts 9 to 11).

Message Submission Envelope: definition of the message-submission-envelope (Figure 2 Part 11).

Probe Submission Envelope: definition of the probe-submission-envelope (Figure 2 Part 12).

Message Delivery Envelope: definition of the message-delivery-envelope (Figure 2 Parts 12 to 13).

Report Delivery Envelope: definition of the report-delivery-envelope (Figure 2 Parts 13 to 14).

Envelope Fields: definitions of envelope fields (Figure 2 Parts 14 to 16).

Extension Fields: definitions of extension-fields (Figure 2 Parts 17 to 22).

Common Parameter Types: definitions of common parameter types (Figure 2 Parts 23 to 29).

NOTE – The module implies a number of changes to the P3 protocol defined in CCITT Recommendation X.411 (1984). These changes are highlighted by means of underlining. For the delivery-control and register operations these changes are shown only in Annex C.

[NOTE – The module applies size constraints to variable-length data types using the SIZE subtyping extension of ASN.1. Violation of a size constraint constitutes a protocol violation.|]

9.1 Extension Mechanism

A mechanism is defined in Figure 2 (part 17) to enable extensions to be defined. Where extensions may appear, a parameterized information object set indicates those extensions defined in this Service Definition which may be present, but other extensions defined elsewhere (e.g., privately, or by addenda or future versions of this Recommendation | International Standard) may also be included.

NOTE 1 – Only extensions defined in ITU-T Rec. X.411 | ISO/IEC 10021-4, and addenda or future versions of ITU-T Rec. X.411 | ISO/IEC 10021-4, may be identified by ExtensionType.standard-extension. All extensions defined elsewhere are identified by ExtensionType.private-extension

Each extension type shall occur at most once in a set of ExtensionField. The same extension type may occur in different places in the protocol. This applies to both standardised extensions and private extensions.

NOTE 2 – Per-message and per-recipient extensions are merged on delivery. This should be considered when defining a private extension.

9.2 Criticality Mechanism

Each **extension-field** defined in Figure 2 (Parts 13 to 18) carries with it an indication of its **criticality** for submission, transfer and delivery. The values of **criticality** may be set when the **extension-field** is generated.

The criticality mechanism is designed to support controlled transparency of extended functions. A non-critical function may be ignored, but shall not be discarded except when delivering or downgrading (see ITU-T Rec. X.419 | ISO/IEC 10021-6 Annex B) a message, while a critical function must be known and performed correctly for normal procedures to continue.

NOTE – Messages with critical or non-critical functions may be rejected on submission with the submission error Element-of-service-not-subscribed when the function corresponds to an element of service to which the user has not subscribed, or which is not available for subscription.

In general, an argument of an abstract-operation marked critical for the port type shall be correctly handled by the performer of the abstract-operation, or an error reported in an appropriate way. The invoker of an abstract-operation shall also correctly handle any functions marked critical for the port type.

If the abstract-operation is one that reports an unsuccessful outcome, failure to correctly perform a critical function is reported by returning an Unsupported-critical-function abstract-error. If an abstract-operation is not one that reports an unsuccessful outcome, an abstract-operation (e.g., a report) shall be invoked to convey the unsuccessful outcome of the previous operation (e.g., using the **unsupported-critical-function non-delivery-diagnostic-code** of a report).

An extension that appears in the result of an abstract-operation shall not be marked critical for the port type.

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

In the case of **critical-for-submission**, the MTS shall correctly perform the procedures defined for a function marked as **critical-for-submission** in a Message-submission or Probe-submission abstract-operation, or shall return an Unsupported-critical-function abstract-error.

In the case of **critical-for-transfer**, a receiving MTA shall correctly perform the procedures defined for a function in a message or probe marked as **critical-for-transfer**, or shall return a non-delivery-report with the **non-delivery-diagnostic-code** set to **unsupported-critical-function**. An MTA unable to support a function marked **critical-for-transfer** in a report shall discard the report (a local policy or agreement may require that this action be audited). An extension marked as **critical-for-transfer** that appears as an argument of a Message-submission or Probe-submission operation shall appear unchanged in a resulting Message-transfer or Probe-transfer operation at a transfer-port.

In the case of **critical-for-delivery**, a delivering-MTA shall correctly perform the procedures defined for a function marked as **critical-for-delivery**, or shall not deliver the message or probe and shall return a non-delivery-report with the **non-delivery-diagnostic-code** set to **unsupported-critical-function**. A recipient MTS-user shall correctly perform the procedures defined for a function marked as **critical-for-delivery** or shall return an Unsupported-critical-function abstract-error. An extension marked as **critical-for-delivery** that appears as an argument of a Message-submission or Probe-submission operation shall appear unchanged in a resulting Message-transfer or Probe-transfer operation at a transfer-port. An extension marked as **critical-for-delivery** that appears as an argument of a Message-transfer or Probe-transfer operation shall appear unchanged in any resulting Message-transfer or Probe-transfer operation at a transfer-port.

An MTA generating a report shall not copy unsupported critical functions from the subject into the report. When generating a report, an MTA shall indicate the **criticality** (for transfer and/or delivery) of any supported functions copied from the subject into the report; the **criticality** of a function in a report may be different from its **criticality** in the subject.

If the MTA or MTS-user cannot correctly perform the procedures defined for a function marked **critical-for-delivery** in a report, then the report shall be discarded.

The procedures related to **extension-fields** and their **criticality** indications are further defined in clause 14.

This Service Definition defines by means of the information object class notation of ASN.1 the recommended setting of the **criticality** indication of **extension-fields** to be supplied by the originator of a message. The originator of a message or probe may choose, on a per-message basis, or in accordance with some local policy (e.g., a security-policy), to set the **criticality** indication of an extension-field to other than that defined in this Service Definition, either to relax or further constrain its **criticality**.

Table 27 identifies the possible alternatives open to an MTA for all the combinations of **criticality**.

Table 27 – MTA Actions on Criticality

Critical for			Submit* Clause 14.6	Front end* Clause 14.3.2	Message delivery* Clause 14.7	Down-grading+
Submission	**Transfer**	**Delivery**				
			A, R, E	A, R	A, R, D	A, D
		x	A, R, E	A, R	A, N	A, N
	x		A, R, E	A, N	A, R, D	A, N
	x	x	A, R, E	A, N	A, N	A, N
x			A, E	A, R	A, R, D	A, D
X		x	A, E	A, R	A, N	A, N

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

Table 27 – MTA Actions on Criticality

Critical for			Submit* Clause 14.6	Front end* Clause 14.3.2	Message delivery* Clause 14.7	Down-grading+
Submission	Transfer	Delivery				
X	x		A, E	A, N	A, R, D	A, N
X	x	x	A, E	A, N	A, N	A, N

Key:
* = See Figures 6 and 7 for these labels
\+ = See ITU-T Rec. X.419 | ISO/IEC 10021-6 Annex B
x = Criticality bit set to *critical*
A = Act on semantics
D = Discard extension and Deliver or Downgrade as applicable
E = submission-Error (element-of-service-not-subscribed)
N = Non-deliver messages or probes, discard reports (unsupported-critical-function)
R = Relay or deliveR as applicable retaining the extension intact, but no action on the semantics

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

Figure 2 – Abstract Syntax Definition of the MTS Abstract Service (Start)

```
--      Figure 2 – Part 1 of 29

MTSAbstractService { joint-iso-itu-t mhs(6) mts(3) modules(0) mts-abstract-service(1)
                     version-1999(1) }

DEFINITIONS IMPLICIT TAGS ::=

BEGIN

--      Prologue

--      Exports everything

IMPORTS

        -- Remote Operations

        CONNECTION-PACKAGE, CONTRACT, ERROR, OPERATION, OPERATION-PACKAGE, ROS-OBJECT-CLASS
                ----
                FROM Remote-Operations-Information-Objects { joint-iso-itu-t
        remote-operations(4)
                     informationObjects(5) version1(0) }

        emptyUnbind
                ----
                FROM Remote-Operations-Useful-Definitions { joint-iso-itu-t remote-operations(4)
                     useful-definitions(7) version1(0) }

        -- MTA Abstract Service

        internal-trace-information, trace-information
                ----
                FROM MTAAbstractService { joint-iso-itu-t mhs(6) mts(3) modules(0)
                     mta-abstract-service(2) version-1999(1) }

        -- MS Abstract Service Extension

        forwarding-request
                ----
                FROM MSAbstractService { joint-iso-itu-t mhs(6) ms(4) modules(0)
                     abstract-service(1) version-1999(1) }

        -- IPM Information Objects

        IPMPerRecipientEnvelopeExtensions
                ----
                FROM IPMSInformationObjects { joint-iso-itu-t mhs(6) ipms(1) modules(0)
                     information-objects(2) version-1999(1) }

        -- Object Identifiers

        id-att-physicalRendition-basic, id-cp-mts-connect, id-ct-mts-access,
        id-ct-mts-forced-access, id-ot-mts, id-ot-mts-user, id-pt-administration,
        id-pt-delivery, id-pt-submission, id-tok-asymmetricToken
                ----
                FROM MTSObjectIdentifiers { joint-iso-itu-t mhs(6) mts(3) modules(0)
                     object-identifiers(0) version-1999(1) }

        -- Operation and Error Codes

        err-control-violates-registration, err-deferred-delivery-cancellation-rejected,
        err-delivery-control-violated, err-element-of-service-not-subscribed,
        err-inconsistent-request, err-message-submission-identifier-invalid,
        err-new-credentials-unacceptable, err-old-credentials-incorrectly-specified,
        err-operation-refused, err-originator-invalid, err-recipient-improperly-specified,
        err-register-rejected, err-remote-bind-error, err-security-error,
        err-submission-control-violated, err-unsupported-critical-function,
        op-cancel-deferred-delivery, op-change-credentials, op-delivery-control,
        op-message-delivery, op-message-submission, op-probe-submission, op-register,
        op-report-delivery, op-submission-control
                ----
                FROM MTSAccessProtocol { joint-iso-itu-t mhs(6) protocols(0) modules(0)
                     mts-access-protocol(1) version-1999(1) }
```


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

```
--      Figure 2 - Part 2 of 29
```

-- Directory Definitions

```
        Name
                ----
                FROM InformationFramework { joint-iso-itu-t ds(5) module(1)
                        informationFramework(1) 3 }

        PresentationAddress
                ----
                FROM SelectedAttributeTypes {joint-iso-itu-t ds(5) module(1)
                        selectedAttributeTypes(5) 3 }

        ALGORITHM, AlgorithmIdentifier, Certificates, ENCRYPTED { }, SIGNATURE { }, SIGNED { }
                ----
                FROM AuthenticationFramework {joint-iso-itu-t ds(5) module(1)
                        authenticationFramework(7) 3 }
```

-- Certificate Extensions

```
        CertificateAssertion
                ----
                FROM CertificateExtensions {joint-iso-itu-t ds(5) module(1)
                        certificateExtensions(26) 0 }
```

-- Upper Bounds

```
        ub-bit-options, ub-built-in-content-type, ub-built-in-encoded-information-types,
        ub-certificates, ub-common-name-length, ub-content-id-length, ub-content-length,
        ub-content-types, ub-country-name-alpha-length, ub-country-name-numeric-length,
        ub-deliverable-class, ub-diagnostic-codes, ub-dl-expansions,
        ub-domain-defined-attributes, ub-domain-defined-attribute-type-length,
        ub-domain-defined-attribute-value-length, ub-domain-name-length,
        ub-encoded-information-types, ub-extension-attributes, ub-extension-types,
        ub-e163-4-number-length, ub-e163-4-sub-address-length, ub-generation-qualifier-length,
        ub-given-name-length, ub-initials-length, ub-integer-options, ub-local-id-length,
        ub-mta-name-length, ub-mts-user-types, ub-numeric-user-id-length,
        ub-organization-name-length, ub-organizational-units,
        ub-organizational-unit-name-length, ub-orig-and-dl-expansions, ub-password-length,
        ub-pds-name-length, ub-pds-parameter-length, ub-pds-physical-address-lines,
        ub-postal-code-length, ub-privacy-mark-length, ub-queue-size, ub-reason-codes,
        ub-recipients, ub-recipient-number-for-advice-length, ub-redirections,
        ub-redirection-classes, ub-restrictions, ub-security-categories, ub-security-labels,
        ub-security-problems, ub-supplementary-info-length, ub-surname-length,
        ub-terminal-id-length, ub-tsap-id-length, ub-unformatted-address-length,
        ub-universal-generation-qualifier-length, ub-universal-given-name-length,
        ub-universal-initials-length, ub-universal-surname-length, ub-x121-address-length
                ----
                FROM MTSUpperBounds { joint-iso-itu-t mhs(6) mts(3) modules(0)
                        upper-bounds(3) version-1999(1) };

        operationObject1 OPERATION ::= {LINKED  {operationObject2}}
        operationObject2 OPERATION ::= {LINKED  {operationObject3}}
        operationObject3 OPERATION ::= {LINKED  {operationObject4}}
        operationObject4 OPERATION ::= {LINKED  {...}}
```

-- Objects

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

mts MHS-OBJECT ::= {
        INITIATES   { mts-forced-access-contract }
        RESPONDS    { mts-access-contract }
        ID          id-ot-mts }

mts-user MHS-OBJECT ::= {
        INITIATES   { mts-access-contract }
        RESPONDS    { mts-forced-access-contract }
        ID          id-ot-mts-user }
```

-- Contracts

```
mts-access-contract CONTRACT ::= {
        CONNECTION              mts-connect
        INITIATOR CONSUMER OF   { submission | delivery | administration }
        ID                      id-ct-mts-access }
```


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

```
--     Figure 2 - Part 2 of 29

mts-forced-access-contract CONTRACT ::= {
       CONNECTION              mts-connect
       RESPONDER CONSUMER OF   { submission | delivery | administration }
       ID                      id-ct-mts-forced-access }
```

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

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

-- Figure 2 – Part 3 of 29

-- Connection package

```
mts-connect CONNECTION-PACKAGE ::= {
       BIND        mts-bind
       UNBIND      mts-unbind
       ID          id-cp-mts-connect }
```

-- Ports

```
PORT ::= OPERATION-PACKAGE

submission PORT ::= {
       OPERATIONS      {operationObject1,...}  /* This information object set has to be
extensible because it is used by Forward{} (as defined in ITU-T Rec. X.880) */
       CONSUMER INVOKES  {message-submission | probe-submission | cancel-deferred-
delivery,...} /* This information object set has to be extensible because it is used by
Forward{} (as defined in ITU-T Rec. X.880) */
       SUPPLIER INVOKES  {submission-control,...} /* This information object set has to be
extensible because it is used by Forward{} (as defined in ITU-T Rec. X.880) */
       ID                id-pt-submission}

delivery PORT ::= {
       OPERATIONS {operationObject1,...} /* This information object set has to be extensible
because it is used by Forward{} (as defined in ITU-T Rec. X.880) */
       CONSUMER INVOKES {delivery-control,...} /* This information object set has to be
extensible because it is used by Forward{} (as defined in ITU-T Rec. X.880) */
       SUPPLIER INVOKES {message-delivery | report-delivery,...} /* This information object
set has to be extensible because it is used by Forward{} (as defined in ITU-T Rec. X.880) */
       ID id-pt-delivery }

administration PORT ::= {
       OPERATIONS {change-credentials,...} /* This information object set has to be extensible
because it is used by Forward{} (as defined in ITU-T Rec. X.880) */
       CONSUMER INVOKES {register,...} /* This information object set has to be extensible
because it is used by Forward{} (as defined in ITU-T Rec. X.880) */
       SUPPLIER INVOKES {operationObject1,...} /* This information object set has to be
extensible because it is used by Forward{} (as defined in ITU-T Rec. X.880) */
       ID id-pt-administration
```

-- MTS-bind and MTS-unbind

```
ABSTRACT-OPERATION ::= OPERATION

ABSTRACT-ERROR ::= ERROR

mts-bind ABSTRACT-OPERATION ::= {
       ARGUMENT    MTSBindArgument
       RESULT      MTSBindResult
       ERRORS      { mts-bind-error } }

MTSBindArgument ::=  SET {
       initiator-name            ObjectName,
       messages-waiting      [1] EXPLICIT MessagesWaiting OPTIONAL,
       initiator-credentials [2] InitiatorCredentials,
       security-context      [3] SecurityContext OPTIONAL,
       ... ,
       extensions            [5] SET OF ExtensionField {{ MTSBindExtensions }} DEFAULT { } }

MTSBindExtensions EXTENSION ::= { PrivateExtensions, ... }
       -- May contain private extensions and future standardised extensions

MTSBindResult ::= SET {
       responder-name            ObjectName,
       messages-waiting      [1] EXPLICIT MessagesWaiting OPTIONAL,
       responder-credentials [2] ResponderCredentials,
       ... ,
       extensions            [3] SET OF ExtensionField {{ MTSBindResultExtensions }}
                                                                    DEFAULT { } }

MTSBindResultExtensions EXTENSION ::= { PrivateExtensions, ... }
       -- May contain private extensions and future standardised extensions
```


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

```
--     Figure 2 - Part 3 of 29

mts-bind-error ABSTRACT-ERROR ::= {
       PARAMETER  INTEGER {
              busy                                  (0),
              authentication-error                  (2),
              unacceptable-dialogue-mode            (3),
              unacceptable-security-context         (4),
              inadequate-association-confidentiality (5) } (0..ub-integer-options) }

mts-unbind ABSTRACT-OPERATION ::= emptyUnbind
```


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

```
--      Figure 2 - Part 4 of 29

--      Association Control Parameters

ObjectName ::= CHOICE {
       user-agent ORAddressAndOptionalDirectoryName,
       mTA [0] MTAName,
       message-store [4] ORAddressAndOptionalDirectoryName}

MessagesWaiting ::= SET {
       urgent [0] DeliveryQueue,
       normal [1] DeliveryQueue,
       non-urgent [2] DeliveryQueue }

DeliveryQueue ::= SET {
       messages [0] INTEGER (0..ub-queue-size),
       octets [1] INTEGER (0..ub-content-length) OPTIONAL }

InitiatorCredentials ::= Credentials

ResponderCredentials ::= Credentials

Credentials ::= CHOICE {
       simple Password,
       strong [0] StrongCredentials,
       ... ,
       protected [1] ProtectedPassword }

Password ::= CHOICE {
       ia5-string IA5String (SIZE (0..ub-password-length)),
       octet-string OCTET STRING (SIZE (0..ub-password-length)) }

StrongCredentials ::= SET {
       bind-token [0] Token OPTIONAL,
       certificate [1] Certificates OPTIONAL,
       ... ,
       certificate-selector [2] CertificateAssertion OPTIONAL }

ProtectedPassword ::= SET {
       signature SIGNATURE { SET {
              password Password,
              time1 [0] UTCTime OPTIONAL,
              time2 [1] UTCTime OPTIONAL,
              random1 [2] BIT STRING OPTIONAL,
              random2 [3] BIT STRING OPTIONAL } },
       time1 [0] UTCTime OPTIONAL,
       time2 [1] UTCTime OPTIONAL,
       random1 [2] BIT STRING OPTIONAL,
       random2 [3] BIT STRING OPTIONAL }

SecurityContext ::= SET SIZE (1..ub-security-labels) OF SecurityLabel

--      Submission Port

message-submission ABSTRACT-OPERATION ::= {
       ARGUMENT          MessageSubmissionArgument
       RESULT            MessageSubmissionResult
       ERRORS            { submission-control-violated |
                           element-of-service-not-subscribed |
                           originator-invalid |
                           recipient-improperly-specified |
                           inconsistent-request |
                           security-error |
                           unsupported-critical-function |
                           remote-bind-error }
       LINKED {operationObject1,...} /* This information object set has to be extensible
because it is used by Forward{} (as defined in ITU-T Rec. X.880) */
       INVOKE-PRIORITY   { 4 | 6 | 7 }
       CODE              op-message-submission }
```


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

```
--      Figure 2 - Part 5 of 29

MessageSubmissionArgument ::= SEQUENCE {
        envelope MessageSubmissionEnvelope,
        content Content }

MessageSubmissionResult ::= SET {
        message-submission-identifier MessageSubmissionIdentifier,
        message-submission-time [0] MessageSubmissionTime,
        content-identifier ContentIdentifier OPTIONAL,
        extensions [1] SET OF ExtensionField {{ MessageSubmissionResultExtensions }}
                                                                    DEFAULT { } }

MessageSubmissionResultExtensions EXTENSION ::= {
        -- May contain the following extensions, private extensions, and future standardised extensions,
        -- at most one instance of each extension type:
        originating-MTA-certificate |
        proof-of-submission |
        PrivateExtensions, ... }

probe-submission ABSTRACT-OPERATION ::= {
        ARGUMENT          ProbeSubmissionArgument
        RESULT            ProbeSubmissionResult
        ERRORS            { submission-control-violated |
                            element-of-service-not-subscribed |
                            originator-invalid |
                            recipient-improperly-specified |
                            inconsistent-request |
                            security-error |
                            unsupported-critical-function |
                            remote-bind-error }
        LINKED {operationObject1,...} /* This information object set has to be extensible
because it is used by Forward{} (as defined in ITU-T Rec. X.880) */
        INVOKE-PRIORITY   { 5 }
        CODE              op-probe-submission }

ProbeSubmissionArgument ::= ProbeSubmissionEnvelope

ProbeSubmissionResult ::= SET {
        probe-submission-identifier ProbeSubmissionIdentifier,
        probe-submission-time [0] ProbeSubmissionTime,
        content-identifier ContentIdentifier OPTIONAL,
        extensions [1] SET OF ExtensionField {{ ProbeResultExtensions }} DEFAULT { } }

ProbeResultExtensions EXTENSION ::= { PrivateExtensions, ... }
        -- May contain private extensions and future standardised extensions,
        -- at most one instance of each extension type

cancel-deferred-delivery ABSTRACT-OPERATION ::= {
        ARGUMENT          CancelDeferredDeliveryArgument
        RESULT            CancelDeferredDeliveryResult
        ERRORS            { deferred-delivery-cancellation-rejected |
                            message-submission-identifier-invalid |
                            remote-bind-error }
        LINKED {operationObject1,...} /* This information object set has to be extensible
because it is used by Forward{} (as defined in ITU-T Rec. X.880) */
        INVOKE-PRIORITY   { 3 }
        CODE              op-cancel-deferred-delivery }

CancelDeferredDeliveryArgument ::= MessageSubmissionIdentifier

CancelDeferredDeliveryResult ::= NULL

submission-control ABSTRACT-OPERATION ::= {
        ARGUMENT          SubmissionControlArgument
        RESULT            SubmissionControlResult
        ERRORS            { security-error | remote-bind-error }
        LINKED {operationObject1,...} /* This information object set has to be extensible
because it is used by Forward{} (as defined in ITU-T Rec. X.880) */
        INVOKE-PRIORITY   { 3 }
        CODE              op-submission-control }

SubmissionControlArgument ::= SubmissionControls

SubmissionControlResult ::= Waiting
```


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

```
--      Figure 2 - Part 6 of 29

submission-control-violated ABSTRACT-ERROR ::= {
       PARAMETER   NULL
       CODE        err-submission-control-violated }

element-of-service-not-subscribed ABSTRACT-ERROR ::= {
       PARAMETER   NULL
       CODE        err-element-of-service-not-subscribed }

deferred-delivery-cancellation-rejected ABSTRACT-ERROR ::= {
       PARAMETER   NULL
       CODE        err-deferred-delivery-cancellation-rejected }

originator-invalid ABSTRACT-ERROR ::= {
       PARAMETER   NULL
       CODE        err-originator-invalid }

recipient-improperly-specified ABSTRACT-ERROR ::= {
       PARAMETER   ImproperlySpecifiedRecipients
       CODE        err-recipient-improperly-specified }

ImproperlySpecifiedRecipients ::= SEQUENCE SIZE (1..ub-recipients) OF RecipientName

message-submission-identifier-invalid ABSTRACT-ERROR ::= {
       PARAMETER   NULL
       CODE        err-message-submission-identifier-invalid }

inconsistent-request ABSTRACT-ERROR ::= {
       PARAMETER   NULL
       CODE        err-inconsistent-request }

security-error ABSTRACT-ERROR ::= {
       PARAMETER   SecurityProblem
       CODE        err-security-error }

SecurityProblem ::= INTEGER {
       assemby-instructions-conflict-with-security-services (0),
       authentication-problem (1),
       authentication-failure-on-subject-message (2),
       confidentiality-association-problem (3),
       decryption-failed (4),
       decryption-key-unobtainable (5),
       failure-of-proof-of-message (6),
       forbidden-user-security-label-register (7),
       incompatible-change-with-original-security-context (8),
       integrity-failure-on-subject-message (9),
       invalid-security-label (10),
       invalid-security-label-update (11),
       key-failure (12),
       mandatory-parameter-absence (13),
       operation-security-failure (14),
       redirection-prohibited (15),
       refused-alternate-recipient-name (16),
       repudiation-failure-of-message (17),
       responder-credentials-checking-problem (18),
       security-context-failure (19),
       security-context-problem (20),
       security-policy-violation (21),
       security-services-refusal (22),
       token-decryption-failed (23),
       token-error (24),
       unable-to-aggregate-security-labels (25),
       unauthorised-dl-name (26),
       unauthorised-entry-class (27),
       unauthorised-originally-intended-recipient-name (28),
       unauthorised-originator-name (29),
       unauthorised-recipient-name (30),
       unauthorised-security-label-update (31),
       unauthorised-user-name (32),
       unknown-security-label (33),
       unsupported-algorithm-identifier (34),
       unsupported-security-policy (35) } (0..ub-security-problems)

unsupported-critical-function ABSTRACT-ERROR ::= {
       PARAMETER   NULL
       CODE        err-unsupported-critical-function }
```


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

```
--      Figure 2 - Part 6 of 29

remote-bind-error ABSTRACT-ERROR ::= {
       PARAMETER   NULL
       CODE        err-remote-bind-error }

--      Submission Port Parameters

MessageSubmissionIdentifier ::= MTSIdentifier

MessageSubmissionTime ::= Time

ProbeSubmissionIdentifier ::= MTSIdentifier

ProbeSubmissionTime ::= Time

SubmissionControls ::= Controls (WITH COMPONENTS {
       ...,
       permissible-content-types ABSENT,
       permissible-encoded-information-types ABSENT })

Waiting ::= SET {
       waiting-operations [0] Operations DEFAULT { },
       waiting-messages [1] WaitingMessages DEFAULT { },
       waiting-content-types [2] SET SIZE (0..ub-content-types) OF ContentType DEFAULT { },
       waiting-encoded-information-types EncodedInformationTypes OPTIONAL }
```

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

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

```
--      Figure 2 - Part 7 of 29

Operations ::= BIT STRING {
       probe-submission-or-report-delivery (0),
       message-submission-or-message-delivery (1) } (SIZE (0..ub-bit-options))
       -- holding 'one', not-holding 'zero'

WaitingMessages ::= BIT STRING {
       long-content (0),
       low-priority (1),
       other-security-labels (2) } (SIZE (0..ub-bit-options))

--      Delivery Port

message-delivery ABSTRACT-OPERATION ::= {
       ARGUMENT          MessageDeliveryArgument
       RESULT            MessageDeliveryResult
       ERRORS            { delivery-control-violated | security-error |
                           unsupported-critical-function }
       LINKED {operationObject1,...} /* This information object set has to be extensible
because it is used by Forward{} (as defined in ITU-T Rec. X.880) */
       INVOKE-PRIORITY   { 4 | 6 | 7 }
       CODE              op-message-delivery }

MessageDeliveryArgument ::= SEQUENCE {
       COMPONENTS OF MessageDeliveryEnvelope,
       content Content }

MessageDeliveryResult ::=  SET {
       recipient-certificate [0] RecipientCertificate OPTIONAL,
       proof-of-delivery [1] IMPLICIT ProofOfDelivery OPTIONAL,
       ... ,
       extensions [2] SET OF ExtensionField {{ MessageDeliveryResultExtensions }} DEFAULT { }}

MessageDeliveryResultExtensions EXTENSION ::= { PrivateExtensions, ... }
       -- May contain private extensions and future standardised extensions

report-delivery ABSTRACT-OPERATION ::= {
       ARGUMENT          ReportDeliveryArgument
       RESULT            ReportDeliveryResult
       ERRORS            { delivery-control-violated | security-error |
                           unsupported-critical-function }
       LINKED {operationObject1,...} /* This information object set has to be extensible
because it is used by Forward{} (as defined in ITU-T Rec. X.880) */
       INVOKE-PRIORITY   { 5 }
       CODE              op-report-delivery }

ReportDeliveryArgument ::= SET {
       COMPONENTS OF ReportDeliveryEnvelope,
       returned-content [0] Content OPTIONAL }

ReportDeliveryResult ::= CHOICE {
       empty-result NULL,
       ... ,
       extensions SET SIZE (1..MAX) OF ExtensionField {{ ReportDeliveryResultExtensions }} }

ReportDeliveryResultExtensions EXTENSION ::= { PrivateExtensions, ... }
       -- May contain private extensions and future standardised extensions

delivery-control ABSTRACT-OPERATION ::= {
       ARGUMENT          DeliveryControlArgument
       RESULT            DeliveryControlResult
       ERRORS            { control-violates-registration | security-error | operation-refused}
       LINKED {operationObject1,...} /* This information object set has to be extensible
because it is used by Forward{} (as defined in ITU-T Rec. X.880) */
       INVOKE-PRIORITY   { 3 }
       CODE              op-delivery-control }

DeliveryControlArgument ::= SET {
       COMPONENTS OF DeliveryControls,
       extensions [6] SET OF ExtensionField {{ DeliveryControlExtensions }} DEFAULT { } }

DeliveryControlExtensions EXTENSION ::= { PrivateExtensions, ... }
       -- May contain private extensions and future standardised extensions
```


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

```
--      Figure 2 - Part 8 of 29


DeliveryControlResult ::= SET {
       COMPONENTS OF Waiting,
       extensions [6] SET OF ExtensionField {{ DeliveryControlResultExtensions }} DEFAULT { }}

DeliveryControlResultExtensions EXTENSION ::= { PrivateExtensions, ... }
       -- May contain private extensions and future standardised extensions

delivery-control-violated ABSTRACT-ERROR ::= {
       PARAMETER   NULL
       CODE        err-delivery-control-violated }

control-violates-registration ABSTRACT-ERROR ::= {
       PARAMETER   NULL
       CODE        err-control-violates-registration }

operation-refused ABSTRACT-ERROR ::= {
       PARAMETER   RefusedOperation
       CODE        err-operation-refused }

RefusedOperation ::= SET {
       refused-argument CHOICE {
              built-in-argument [1] RefusedArgument,
              refused-extension EXTENSION.&id },
       refusal-reason [2] RefusalReason }

RefusedArgument ::= INTEGER {
       user-name (0),
       user-address (1),
       deliverable-content-types (2),
       deliverable-maximum-content-length (3),
       deliverable-encoded-information-types-constraints (4),
       deliverable-security-labels (5),
       recipient-assigned-redirections (6),
       restricted-delivery (7),
       retrieve-registrations (8), -- value 9 reserved for possible future extension to Register arguments
       restrict (10),
       permissible-operations (11),
       permissible-lowest-priority (12),
       permissible-encoded-information-types (13),
       permissible-content-types (14),
       permissible-maximum-content-length (15),
       permissible-security-context (16) } (0..ub-integer-options)

RefusalReason ::= INTEGER {
       facility-unavailable (0),
       facility-not-subscribed (1),
       parameter-unacceptable (2) } (0..ub-integer-options)

--      Delivery Port Parameters

RecipientCertificate ::= Certificates

ProofOfDelivery ::= SIGNATURE { SEQUENCE {
       algorithm-identifier ProofOfDeliveryAlgorithmIdentifier,
       delivery-time MessageDeliveryTime,
       this-recipient-name ThisRecipientName,
       originally-intended-recipient-name OriginallyIntendedRecipientName OPTIONAL,
       content Content,
       content-identifier ContentIdentifier OPTIONAL,
       message-security-label MessageSecurityLabel OPTIONAL } }

ProofOfDeliveryAlgorithmIdentifier ::= AlgorithmIdentifier

DeliveryControls ::= Controls
```


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

```
--      Figure 2 – Part 9 of 29


Controls ::= SET {
       restrict [0] BOOLEAN DEFAULT TRUE,
       -- update 'TRUE', remove 'FALSE'
       permissible-operations [1] Operations OPTIONAL,
       permissible-maximum-content-length [2] ContentLength OPTIONAL,
       permissible-lowest-priority Priority OPTIONAL,
       permissible-content-types [4] ContentTypes OPTIONAL,
       permissible-encoded-information-types PermissibleEncodedInformationTypes OPTIONAL,
       permissible-security-context [5] SecurityContext OPTIONAL }

--      Note – The Tags [0], [1] and [2] are altered for the Register operation only.

PermissibleEncodedInformationTypes ::= EncodedInformationTypesConstraints

--      Administration Port

register ABSTRACT-OPERATION ::= {
       ARGUMENT          RegisterArgument
       RESULT            RegisterResult
       ERRORS            { register-rejected | remote-bind-error | operation-refused |
                           security-error }
       LINKED {operationObject1,...} /* This information object set has to be extensible
because it is used by Forward{} (as defined in ITU-T Rec. X.880) */
       INVOKE-PRIORITY   { 5 }
       CODE              op-register }

RegisterArgument ::= SET {
       user-name UserName OPTIONAL,
       user-address [0] UserAddress OPTIONAL,
       deliverable-class SET SIZE (1..ub-deliverable-class) OF DeliverableClass OPTIONAL,
       default-delivery-controls [2] EXPLICIT DefaultDeliveryControls OPTIONAL,
       redirections [3] Redirections OPTIONAL,
       restricted-delivery [4] RestrictedDelivery OPTIONAL,
       retrieve-registrations [5] RegistrationTypes OPTIONAL,
       extensions [6] SET OF ExtensionField {{ RegisterExtensions }} DEFAULT { } }

RegisterExtensions EXTENSION ::= { PrivateExtensions, ... }
       -- May contain private extensions and future standardised extensions

RegisterResult ::= CHOICE {
       empty-result NULL,
       non-empty-result SET {
              registered-information [0] RegisterArgument (WITH COMPONENTS {
                     ... ,
                     retrieve-registrations ABSENT} ) OPTIONAL,
              extensions [1] SET OF ExtensionField {{ RegisterResultExtensions }} DEFAULT {}}}

RegisterResultExtensions EXTENSION ::= { PrivateExtensions, ... }
       -- May contain private extensions and future standardised extensions

change-credentials ABSTRACT-OPERATION ::= {
       ARGUMENT          ChangeCredentialsArgument
       RESULT            NULL
       ERRORS            { new-credentials-unacceptable |
old-credentials-incorrectly-specified |
                           remote-bind-error | security-error }
       LINKED {operationObject1,...} /* This information object set has to be extensible
because it is used by Forward{} (as defined in ITU-T Rec. X.880) */
       INVOKE-PRIORITY   { 5 }
       CODE              op-change-credentials }

ChangeCredentialsArgument ::= SET {
       old-credentials [0] Credentials (WITH COMPONENTS { simple }),
       new-credentials [1] Credentials (WITH COMPONENTS { simple }) }

register-rejected ABSTRACT-ERROR ::= {
       PARAMETER   NULL
       CODE        err-register-rejected }

new-credentials-unacceptable ABSTRACT-ERROR ::= {
       PARAMETER   NULL
       CODE        err-new-credentials-unacceptable }
```


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

```
--      Figure 2 - Part 10 of 29

old-credentials-incorrectly-specified ABSTRACT-ERROR ::= {
       PARAMETER   NULL
       CODE        err-old-credentials-incorrectly-specified }

--      Administration Port Parameters

UserName ::= ORAddressAndOptionalDirectoryName

UserAddress ::= CHOICE {
       x121 [0] SEQUENCE {
              x121-address NumericString (SIZE (1..ub-x121-address-length)) OPTIONAL,
              tsap-id PrintableString (SIZE (1..ub-tsap-id-length)) OPTIONAL },
       presentation [1] PSAPAddress }

PSAPAddress ::= PresentationAddress

DeliverableClass ::= MessageClass (WITH COMPONENTS  {
       ... ,
       priority ABSENT,
       objects ABSENT,
       applies-only-to ABSENT })

DefaultDeliveryControls ::= Controls (WITH COMPONENTS {
       ... ,
       restrict ABSENT,
       permissible-security-context ABSENT })

Redirections ::= SEQUENCE SIZE (1..ub-redirections) OF RecipientRedirection

RecipientRedirection ::= SET {
       redirection-classes [0] SET SIZE (1..ub-redirection-classes) OF RedirectionClass
                                                                              OPTIONAL,
       recipient-assigned-alternate-recipient [1] RecipientAssignedAlternateRecipient
                                                                              OPTIONAL }

RedirectionClass ::=  MessageClass

MessageClass ::= SET {
       content-types [0] ContentTypes OPTIONAL,
       maximum-content-length [1] ContentLength OPTIONAL,
       encoded-information-types-constraints [2] EncodedInformationTypesConstraints OPTIONAL,
       security-labels [3] SecurityContext OPTIONAL,
       priority [4] SET OF Priority OPTIONAL,
       objects [5] ENUMERATED { messages (0), reports (1), both (2), ... } DEFAULT both,
       applies-only-to [6] SEQUENCE OF Restriction OPTIONAL, -- Not considered in the case of Reports --
       extensions [7] SET OF ExtensionField {{ MessageClassExtensions }} DEFAULT { } }

EncodedInformationTypesConstraints ::= SEQUENCE {
       unacceptable-eits           [0] ExtendedEncodedInformationTypes OPTIONAL,
       acceptable-eits             [1] ExtendedEncodedInformationTypes OPTIONAL,
       exclusively-acceptable-eits [2] ExtendedEncodedInformationTypes OPTIONAL }

MessageClassExtensions EXTENSION ::= { PrivateExtensions, ... }
       -- May contain private extensions and future standardised extensions

RecipientAssignedAlternateRecipient ::= ORAddressAndOrDirectoryName

RestrictedDelivery ::=  SEQUENCE SIZE (1..ub-restrictions) OF Restriction

Restriction ::= SET {
       permitted BOOLEAN DEFAULT TRUE,
       source-type BIT STRING {
              originated-by (0),
              redirected-by (1),
              dl-expanded-by (2) } DEFAULT { originated-by, redirected-by, dl-expanded-by },
       source-name ExactOrPattern OPTIONAL }

ExactOrPattern ::= CHOICE {
       exact-match [0] ORName,
       pattern-match [1] ORName }
```


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

```
--      Figure 2 - Part 11 of 29

RegistrationTypes ::=  SEQUENCE {
       standard-parameters [0] BIT STRING {
              user-name (0),
              user-address (1),
              deliverable-class (2),
              default-delivery-controls (3),
              redirections (4),
              restricted-delivery (5) } OPTIONAL,
       extensions [1] SET OF EXTENSION.&id ({ RegisterExtensions }) OPTIONAL }

--      Message Submission Envelope

MessageSubmissionEnvelope ::= SET {
       COMPONENTS OF PerMessageSubmissionFields,
       per-recipient-fields [1] SEQUENCE SIZE (1..ub-recipients) OF
              PerRecipientMessageSubmissionFields }

PerMessageSubmissionFields ::= SET {
       originator-name OriginatorName,
       original-encoded-information-types OriginalEncodedInformationTypes OPTIONAL,
       content-type ContentType,
       content-identifier ContentIdentifier OPTIONAL,
       priority Priority DEFAULT normal,
       per-message-indicators PerMessageIndicators DEFAULT { },
       deferred-delivery-time [0] DeferredDeliveryTime OPTIONAL,
       extensions [2] SET OF ExtensionField {{ PerMessageSubmissionExtensions }} DEFAULT { } }

PerMessageSubmissionExtensions EXTENSION ::= {
       -- May contain the following extensions, private extensions, and future standardised extensions,
       -- at most one instance of each extension type:
       recipient-reassignment-prohibited |
       dl-expansion-prohibited |
       conversion-with-loss-prohibited |
       latest-delivery-time |
       originator-return-address |
       originator-certificate |
       content-confidentiality-algorithm-identifier |
       message-origin-authentication-check |
       message-security-label |
       proof-of-submission-request |
       content-correlator |
       dl-exempted-recipients |
       certificate-selectors |
       multiple-originator-certificates |
       forwarding-request -- for MS Abstract Service only -- |
       PrivateExtensions, ... }

PerRecipientMessageSubmissionFields ::= SET {
       recipient-name RecipientName,
       originator-report-request [0] OriginatorReportRequest,
       explicit-conversion [1] ExplicitConversion OPTIONAL,
       extensions [2] SET OF ExtensionField {{ PerRecipientMessageSubmissionExtensions }}
              DEFAULT { } }

PerRecipientMessageSubmissionExtensions EXTENSION ::= {
       -- May contain the following extensions, private extensions, and future standardised extensions,
       -- at most one instance of each extension type:
       originator-requested-alternate-recipient |
       requested-delivery-method |
       physical-forwarding-prohibited |
       physical-forwarding-address-request |
       physical-delivery-modes |
       registered-mail-type |
       recipient-number-for-advice |
       physical-rendition-attributes |
       physical-delivery-report-request |
       message-token |
       content-integrity-check |
       proof-of-delivery-request |
       certificate-selectors-override |
       recipient-certificate |
       IPMPerRecipientEnvelopeExtensions |
       PrivateExtensions, ... }
```


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

```
--      Figure 2 - Part 12 of 29

--      Probe Submission Envelope

ProbeSubmissionEnvelope ::= SET {
        COMPONENTS OF PerProbeSubmissionFields,
        per-recipient-fields [3] SEQUENCE SIZE (1..ub-recipients) OF
                PerRecipientProbeSubmissionFields }

PerProbeSubmissionFields ::= SET {
        originator-name OriginatorName,
        original-encoded-information-types OriginalEncodedInformationTypes OPTIONAL,
        content-type ContentType,
        content-identifier ContentIdentifier OPTIONAL,
        content-length [0] ContentLength OPTIONAL,
        per-message-indicators PerMessageIndicators DEFAULT { },
        extensions [2] SET OF ExtensionField {{ PerProbeSubmissionExtensions }} DEFAULT { } }

PerProbeSubmissionExtensions EXTENSION ::= {
        -- May contain the following extensions, private extensions, and future standardised extensions,
        -- at most one instance of each extension type:
        recipient-reassignment-prohibited |
        dl-expansion-prohibited |
        conversion-with-loss-prohibited |
        originator-certificate |
        message-security-label |
        content-correlator |
        probe-origin-authentication-check |
        PrivateExtensions, ... }

PerRecipientProbeSubmissionFields ::= SET {
        recipient-name RecipientName,
        originator-report-request [0] OriginatorReportRequest,
        explicit-conversion [1] ExplicitConversion OPTIONAL,
        extensions [2] SET OF ExtensionField {{ PerRecipientProbeSubmissionExtensions }}
                                                                        DEFAULT { } }

PerRecipientProbeSubmissionExtensions EXTENSION ::= {
        -- May contain the following extensions, private extensions, and future standardised extensions,
        -- at most one instance of each extension type:
        originator-requested-alternate-recipient |
        requested-delivery-method |
        physical-rendition-attributes |
        PrivateExtensions, ... }

--      Message Delivery Envelope

MessageDeliveryEnvelope ::= SEQUENCE {
        message-delivery-identifier MessageDeliveryIdentifier,
        message-delivery-time MessageDeliveryTime,
        other-fields OtherMessageDeliveryFields }

OtherMessageDeliveryFields ::= SET {
        content-type DeliveredContentType,
        originator-name DeliveredOriginatorName,
        original-encoded-information-types [1] OriginalEncodedInformationTypes OPTIONAL,
        priority Priority DEFAULT normal,
        delivery-flags [2] DeliveryFlags OPTIONAL,
        other-recipient-names [3] OtherRecipientNames OPTIONAL,
        this-recipient-name [4] ThisRecipientName,
        originally-intended-recipient-name [5] OriginallyIntendedRecipientName OPTIONAL,
        converted-encoded-information-types [6] ConvertedEncodedInformationTypes OPTIONAL,
        message-submission-time [7] MessageSubmissionTime,
        content-identifier [8] ContentIdentifier OPTIONAL,
        extensions [9] SET OF ExtensionField {{ MessageDeliveryExtensions }} DEFAULT { } }
```


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

```
--      Figure 2 - Part 13 of 29

MessageDeliveryExtensions EXTENSION ::= {
        -- May contain the following extensions, private extensions, and future standardised extensions,
        -- at most one instance of each extension type:
        conversion-with-loss-prohibited |
        requested-delivery-method |
        physical-forwarding-prohibited |
        physical-forwarding-address-request |
        physical-delivery-modes |
        registered-mail-type |
        recipient-number-for-advice |
        physical-rendition-attributes |
        originator-return-address |
        physical-delivery-report-request |
        originator-certificate |
        message-token |
        content-confidentiality-algorithm-identifier |
        content-integrity-check |
        message-origin-authentication-check |
        message-security-label |
        proof-of-delivery-request |
        dl-exempted-recipients |
        certificate-selectors |
        certificate-selectors-override |
        multiple-originator-certificates |
        recipient-certificate |
        IPMPerRecipientEnvelopeExtensions |
        redirection-history |
        dl-expansion-history |
        trace-information |
        internal-trace-information |
        PrivateExtensions, ... }

--      Report Delivery Envelope

ReportDeliveryEnvelope ::= SET {
        COMPONENTS OF PerReportDeliveryFields,
        per-recipient-fields SEQUENCE SIZE (1..ub-recipients) OF
                                                PerRecipientReportDeliveryFields }

PerReportDeliveryFields ::= SET {
        subject-submission-identifier SubjectSubmissionIdentifier,
        content-identifier ContentIdentifier OPTIONAL,
        content-type ContentType OPTIONAL,
        original-encoded-information-types OriginalEncodedInformationTypes OPTIONAL,
        extensions [1] SET OF ExtensionField {{ ReportDeliveryExtensions }} DEFAULT { } }

ReportDeliveryExtensions EXTENSION ::= {
        -- May contain the following extensions, private extensions, and future standardised extensions,
        -- at most one instance of each extension type:
        message-security-label |
        content-correlator |
        redirection-history |
        originator-and-DL-expansion-history |
        reporting-DL-name |
        reporting-MTA-certificate |
        report-origin-authentication-check |
        trace-information |
        internal-trace-information |
        reporting-MTA-name |
        PrivateExtensions, ... }

PerRecipientReportDeliveryFields ::= SET {
        actual-recipient-name [0] ActualRecipientName,
        report-type [1] ReportType,
        converted-encoded-information-types ConvertedEncodedInformationTypes OPTIONAL,
        originally-intended-recipient-name [2] OriginallyIntendedRecipientName OPTIONAL,
        supplementary-information [3] SupplementaryInformation OPTIONAL,
        extensions [4] SET OF ExtensionField {{ PerRecipientReportDeliveryExtensions }}
                                                                        DEFAULT { } }

PerRecipientReportDeliveryExtensions EXTENSION ::= {
        -- May contain the following extensions, private extensions, and future standardised extensions,
        -- at most one instance of each extension type:
        redirection-history |
        physical-forwarding-address |
        recipient-certificate |
        proof-of-delivery |
        PrivateExtensions, ... }
```


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

```
--      Figure 2 - Part 14 of 29

ReportType ::= CHOICE {
       delivery [0] DeliveryReport,
       non-delivery [1] NonDeliveryReport }

DeliveryReport ::= SET {
       message-delivery-time [0] MessageDeliveryTime,
       type-of-MTS-user [1] TypeOfMTSUser DEFAULT public }

NonDeliveryReport ::= SET {
       non-delivery-reason-code [0] NonDeliveryReasonCode,
       non-delivery-diagnostic-code [1] NonDeliveryDiagnosticCode OPTIONAL }

--      Envelope Fields

OriginatorName ::= ORAddressAndOrDirectoryName

DeliveredOriginatorName ::= ORAddressAndOptionalDirectoryName

OriginalEncodedInformationTypes ::= EncodedInformationTypes

ContentTypes ::= SET SIZE (1..ub-content-types) OF ContentType

ContentType ::= CHOICE {
       built-in BuiltInContentType,
       extended ExtendedContentType }

BuiltInContentType ::= [APPLICATION 6] INTEGER {
       unidentified (0),
       external (1),                -- identified by the object-identifier of the EXTERNAL content
       interpersonal-messaging-1984 (2),
       interpersonal-messaging-1988 (22),
       edi-messaging (35),
       voice-messaging (40) } (0..ub-built-in-content-type)

ExtendedContentType ::= OBJECT IDENTIFIER

DeliveredContentType ::= CHOICE {
       built-in [0] BuiltInContentType,
       extended ExtendedContentType }

ContentIdentifier ::= [APPLICATION 10] PrintableString (SIZE (1..ub-content-id-length))

PerMessageIndicators ::= [APPLICATION 8] BIT STRING {
       disclosure-of-other-recipients (0), -- disclosure-of-other-recipients-requested 'one',
                                           -- disclosure-of-other-recipients-prohibited 'zero';
                                           -- ignored for Probe-submission
       implicit-conversion-prohibited (1), -- implicit-conversion-prohibited 'one',
                                           -- implicit-conversion-allowed 'zero'
       alternate-recipient-allowed (2),            -- alternate-recipient-allowed 'one',
                                           -- alternate-recipient-prohibited 'zero'
       content-return-request (3),         -- content-return-requested 'one',
                                           -- content-return-not-requested 'zero';
                                           -- ignored for Probe-submission
       reserved (4),                       -- bit reserved by MOTIS 1986
       bit-5 (5),
       bit-6 (6),                          -- notification type-1 : bit 5 'zero' and bit 6 'one'
                                           -- notification type-2 : bit 5 'one' and bit 6 'zero'
                                           -- notification type-3 : bit 5 'one' and bit 6 'one'
                                           -- the mapping between notification type 1, 2, 3
                                           -- and the content specific notification types are defined
                                           -- in relevant content specifications
       service-message (7)                 -- the message content is for service purposes;
                                           -- it may be a notification related to a service message;
                                           -- used only by bilateral agreement -- }
       (SIZE (0..ub-bit-options))

RecipientName ::= ORAddressAndOrDirectoryName
```


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

```
--      Figure 2 - Part 15 of 29

OriginatorReportRequest ::= BIT STRING {
       report (3),
       non-delivery-report (4)
       -- at most one bit shall be 'one':
       -- report bit 'one' requests a 'report';
       -- non-delivery-report bit 'one' requests a 'non-delivery-report';
       -- both bits 'zero' requests 'no-report' --  } (SIZE (0..ub-bit-options))

ExplicitConversion ::= INTEGER {
       ia5-text-to-teletex (0),
       -- values 1 to 7 are no longer defined
       ia5-text-to-g3-facsimile (8),
       ia5-text-to-g4-class-1 (9),
       ia5-text-to-videotex (10),
       teletex-to-ia5-text (11),
       teletex-to-g3-facsimile (12),
       teletex-to-g4-class-1 (13),
       teletex-to-videotex (14),
       -- value 15 is no longer defined
       videotex-to-ia5-text (16),
       videotex-to-teletex (17) } (0..ub-integer-options)

DeferredDeliveryTime ::= Time

Priority ::= [APPLICATION 7] ENUMERATED {
       normal (0),
       non-urgent  (1),
       urgent (2) }

ContentLength ::= INTEGER (0..ub-content-length)

MessageDeliveryIdentifier ::= MTSIdentifier

MessageDeliveryTime ::= Time

DeliveryFlags ::= BIT STRING {
       implicit-conversion-prohibited (1)  -- implicit-conversion-prohibited 'one',
                                           -- implicit-conversion-allowed 'zero' --  }
       (SIZE (0..ub-bit-options))

OtherRecipientNames ::= SEQUENCE SIZE (1..ub-recipients) OF OtherRecipientName

OtherRecipientName ::= ORAddressAndOptionalDirectoryName

ThisRecipientName ::= ORAddressAndOptionalDirectoryName

OriginallyIntendedRecipientName ::= ORAddressAndOptionalDirectoryName

ConvertedEncodedInformationTypes ::= EncodedInformationTypes

SubjectSubmissionIdentifier ::= MTSIdentifier

ActualRecipientName ::= ORAddressAndOrDirectoryName

TypeOfMTSUser ::= INTEGER {
       public (0),
       private (1),
       ms (2),
       dl (3),
       pdau (4),
       physical-recipient (5),
       other (6) } (0..ub-mts-user-types)
```


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

```
--      Figure 2 - Part 16 of 29

NonDeliveryReasonCode ::= INTEGER {
        transfer-failure (0),
        unable-to-transfer (1),
        conversion-not-performed (2),
        physical-rendition-not-performed (3),
        physical-delivery-not-performed (4),
        restricted-delivery (5),
        directory-operation-unsuccessful (6),
        deferred-delivery-not-performed (7),
        transfer-failure-for-security-reason (8) } (0..ub-reason-codes)

NonDeliveryDiagnosticCode ::= INTEGER {
        unrecognised-OR-name (0),
        ambiguous-OR-name (1),
        mts-congestion (2),
        loop-detected (3),
        recipient-unavailable (4),
        maximum-time-expired (5),
        encoded-information-types-unsupported (6),
        content-too-long (7),
        conversion-impractical (8),
        implicit-conversion-prohibited (9),
        implicit-conversion-not-subscribed (10),
        invalid-arguments (11),
        content-syntax-error (12),
        size-constraint-violation (13),
        protocol-violation (14),
        content-type-not-supported (15),
        too-many-recipients (16),
        no-bilateral-agreement (17),
        unsupported-critical-function (18),
        conversion-with-loss-prohibited (19),
        line-too-long (20),
        page-split (21),
        pictorial-symbol-loss (22),
        punctuation-symbol-loss (23),
        alphabetic-character-loss (24),
        multiple-information-loss (25),
        recipient-reassignment-prohibited (26),
        redirection-loop-detected (27),
        dl-expansion-prohibited (28),
        no-dl-submit-permission (29),
        dl-expansion-failure (30),
        physical-rendition-attributes-not-supported (31),
        undeliverable-mail-physical-delivery-address-incorrect (32),
        undeliverable-mail-physical-delivery-office-incorrect-or-invalid (33),
        undeliverable-mail-physical-delivery-address-incomplete (34),
        undeliverable-mail-recipient-unknown (35),
        undeliverable-mail-recipient-deceased (36),
        undeliverable-mail-organization-expired (37),
        undeliverable-mail-recipient-refused-to-accept (38),
        undeliverable-mail-recipient-did-not-claim (39),
        undeliverable-mail-recipient-changed-address-permanently (40),
        undeliverable-mail-recipient-changed-address-temporarily (41),
        undeliverable-mail-recipient-changed-temporary-address (42),
        undeliverable-mail-new-address-unknown (43),
        undeliverable-mail-recipient-did-not-want-forwarding (44),
        undeliverable-mail-originator-prohibited-forwarding (45),
        secure-messaging-error (46),
        unable-to-downgrade (47),
        unable-to-complete-transfer (48),
        transfer-attempts-limit-reached (49),
        incorrect-notification-type (50),
        dl-expansion-prohibited-by-security-policy (51),
        forbidden-alternate-recipient (52),
        security-policy-violation (53),
        security-services-refusal (54),
        unauthorised-dl-member (55),
        unauthorised-dl-name (56),
        unauthorised-originally-intended-recipient-name (57),
        unauthorised-originator-name (58),
        unauthorised-recipient-name (59),
        unreliable-system (60),
        authentication-failure-on-subject-message (61),
```

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

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

```
--      Figure 2 - Part 16 of 29

        decryption-failed (62),
        decryption-key-unobtainable (63),
        double-envelope-creation-failure (64),
        double-enveloping-message-restoring-failure (65),
        failure-of-proof-of-message (66),
        integrity-failure-on-subject-message (67),
        invalid-security-label (68),
        key-failure (69),
        mandatory-parameter-absence (70),
        operation-security-failure (71),
        repudiation-failure-of-message (72),
        security-context-failure (73),
        token-decryption-failed (74),
        token-error (75),
        unknown-security-label (76),
        unsupported-algorithm-identifier (77),
        unsupported-security-policy (78) } (0..ub-diagnostic-codes)

SupplementaryInformation ::= PrintableString (SIZE (1..ub-supplementary-info-length))
```


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

```
--      Figure 2 - Part 17 of 29

--      Extension Fields

EXTENSION ::= CLASS {
        &id ExtensionType UNIQUE,
        &Type OPTIONAL,
        &absent &Type OPTIONAL,
        &recommended Criticality DEFAULT { } }
WITH SYNTAX {
        [&Type [IF ABSENT &absent],]
        [RECOMMENDED CRITICALITY &recommended,]
        IDENTIFIED BY &id }

ExtensionType ::= CHOICE {
        standard-extension [0] INTEGER (0..ub-extension-types),
        private-extension [3] OBJECT IDENTIFIER }

Criticality ::= BIT STRING {
        for-submission (0),
        for-transfer (1),
        for-delivery (2) } (SIZE (0..ub-bit-options))     -- critical 'one', non-critical 'zero'

ExtensionField {EXTENSION:ChosenFrom} ::= SEQUENCE {
        type EXTENSION.&id({ChosenFrom}),
        criticality [1] Criticality DEFAULT { },
        value [2] EXTENSION.&Type({ChosenFrom} {@type}) DEFAULT NULL:NULL }

PrivateExtensions EXTENSION ::= {
        -- Any value shall be relayed and delivered if not Critical (see Table 27)
        -- except those values whose semantics the MTA obeys which are defined to be removed when obeyed.
        -- Shall be IDENTIFIED BY ExtensionType.private-extension --  . . .  }

recipient-reassignment-prohibited EXTENSION ::= {
        RecipientReassignmentProhibited IF ABSENT recipient-reassignment-allowed,
        RECOMMENDED CRITICALITY {for-delivery},
        IDENTIFIED BY standard-extension:1 }

RecipientReassignmentProhibited ::= ENUMERATED {
        recipient-reassignment-allowed (0),
        recipient-reassignment-prohibited (1) }

originator-requested-alternate-recipient EXTENSION ::= {
        OriginatorRequestedAlternateRecipient,
        RECOMMENDED CRITICALITY {for-submission},
        IDENTIFIED BY standard-extension:2 }

OriginatorRequestedAlternateRecipient ::= ORAddressAndOrDirectoryName
-- OriginatorRequestedAlternateRecipient as defined here differs from the field of the same name
-- defined in Figure 4, since on submission the OR-address need not be present, but on
-- transfer the OR-address must be present.

dl-expansion-prohibited EXTENSION ::= {
        DLExpansionProhibited IF ABSENT dl-expansion-allowed,
        RECOMMENDED CRITICALITY {for-delivery},
        IDENTIFIED BY standard-extension:3 }

DLExpansionProhibited ::= ENUMERATED {
        dl-expansion-allowed (0),
        dl-expansion-prohibited (1) }

conversion-with-loss-prohibited EXTENSION ::= {
        ConversionWithLossProhibited IF ABSENT conversion-with-loss-allowed,
        RECOMMENDED CRITICALITY {for-delivery},
        IDENTIFIED BY standard-extension:4 }
```


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

```
--      Figure 2 - Part 18 of 29

ConversionWithLossProhibited ::= ENUMERATED {
       conversion-with-loss-allowed (0),
       conversion-with-loss-prohibited (1) }

latest-delivery-time EXTENSION ::= {
       LatestDeliveryTime,
       RECOMMENDED CRITICALITY {for-delivery},
       IDENTIFIED BY standard-extension:5 }

LatestDeliveryTime ::= Time

requested-delivery-method EXTENSION ::= {
       RequestedDeliveryMethod IF ABSENT { any-delivery-method },
       IDENTIFIED BY standard-extension:6 }

RequestedDeliveryMethod ::= SEQUENCE OF INTEGER { -- each different in order of preference,
                                                  -- most preferred first
       any-delivery-method (0),
       mhs-delivery (1),
       physical-delivery (2),
       telex-delivery (3),
       teletex-delivery (4),
       g3-facsimile-delivery (5),
       g4-facsimile-delivery (6),
       ia5-terminal-delivery (7),
       videotex-delivery (8),
       telephone-delivery (9) } (0..ub-integer-options)

physical-forwarding-prohibited EXTENSION ::= {
       PhysicalForwardingProhibited IF ABSENT physical-forwarding-allowed,
       RECOMMENDED CRITICALITY {for-delivery},
       IDENTIFIED BY standard-extension:7 }

PhysicalForwardingProhibited ::= ENUMERATED {
       physical-forwarding-allowed (0),
       physical-forwarding-prohibited (1) }

physical-forwarding-address-request EXTENSION ::= {
       PhysicalForwardingAddressRequest IF ABSENT physical-forwarding-address-not-requested,
       RECOMMENDED CRITICALITY {for-delivery},
       IDENTIFIED BY standard-extension:8 }

PhysicalForwardingAddressRequest ::= ENUMERATED {
       physical-forwarding-address-not-requested (0),
       physical-forwarding-address-requested (1) }

physical-delivery-modes EXTENSION ::= {
       PhysicalDeliveryModes IF ABSENT ordinary-mail,
       RECOMMENDED CRITICALITY {for-delivery},
       IDENTIFIED BY standard-extension:9 }

PhysicalDeliveryModes ::= BIT STRING {
       ordinary-mail (0),
       special-delivery (1),
       express-mail (2),
       counter-collection (3),
       counter-collection-with-telephone-advice (4),
       counter-collection-with-telex-advice (5),
       counter-collection-with-teletex-advice (6),
       bureau-fax-delivery (7)
       -- bits 0 to 6 are mutually exclusive
       -- bit 7 can be set independently of any of bits 0 to 6 -- } (SIZE (0..ub-bit-options))
```


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

```
--      Figure 2 - Part 19 of 29

registered-mail-type EXTENSION ::= {
       RegisteredMailType IF ABSENT non-registered-mail,
       RECOMMENDED CRITICALITY {for-delivery},
       IDENTIFIED BY standard-extension:10 }

RegisteredMailType ::= INTEGER {
       non-registered-mail (0),
       registered-mail (1),
       registered-mail-to-addressee-in-person (2) } (0..ub-integer-options)

recipient-number-for-advice EXTENSION ::= {
       RecipientNumberForAdvice,
       RECOMMENDED CRITICALITY {for-delivery},
       IDENTIFIED BY standard-extension:11 }

RecipientNumberForAdvice ::= TeletexString (SIZE (1..ub-recipient-number-for-advice-length))

physical-rendition-attributes EXTENSION ::= {
       PhysicalRenditionAttributes IF ABSENT id-att-physicalRendition-basic,
       RECOMMENDED CRITICALITY {for-delivery},
       IDENTIFIED BY standard-extension:12 }

PhysicalRenditionAttributes ::= OBJECT IDENTIFIER

originator-return-address EXTENSION ::= {
       OriginatorReturnAddress,
       IDENTIFIED BY standard-extension:13 }

OriginatorReturnAddress ::= ORAddress

physical-delivery-report-request EXTENSION ::= {
       PhysicalDeliveryReportRequest IF ABSENT return-of-undeliverable-mail-by-PDS,
       RECOMMENDED CRITICALITY {for-delivery},
       IDENTIFIED BY standard-extension:14 }

PhysicalDeliveryReportRequest ::= INTEGER {
       return-of-undeliverable-mail-by-PDS (0),
       return-of-notification-by-PDS (1),
       return-of-notification-by-MHS (2),
       return-of-notification-by-MHS-and-PDS (3) } (0..ub-integer-options)

originator-certificate EXTENSION ::= {
       OriginatorCertificate,
       IDENTIFIED BY standard-extension:15 }

OriginatorCertificate ::= Certificates

message-token EXTENSION ::= {
       MessageToken,
       RECOMMENDED CRITICALITY {for-delivery},
       IDENTIFIED BY standard-extension:16 }

MessageToken ::= Token

content-confidentiality-algorithm-identifier EXTENSION ::= {
       ContentConfidentialityAlgorithmIdentifier,
       RECOMMENDED CRITICALITY {for-delivery},
       IDENTIFIED BY standard-extension:17 }

ContentConfidentialityAlgorithmIdentifier ::= AlgorithmIdentifier
```


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

```
--      Figure 2 - Part 20 of 29

content-integrity-check EXTENSION ::= {
       ContentIntegrityCheck,
       RECOMMENDED CRITICALITY {for-delivery},
       IDENTIFIED BY standard-extension:18 }

ContentIntegrityCheck ::= SIGNATURE { SEQUENCE {
       algorithm-identifier ContentIntegrityAlgorithmIdentifier OPTIONAL,
       content Content } }

ContentIntegrityAlgorithmIdentifier ::= AlgorithmIdentifier

message-origin-authentication-check EXTENSION ::= {
       MessageOriginAuthenticationCheck,
       RECOMMENDED CRITICALITY {for-delivery},
       IDENTIFIED BY standard-extension:19 }

MessageOriginAuthenticationCheck ::= SIGNATURE { SEQUENCE {
       algorithm-identifier MessageOriginAuthenticationAlgorithmIdentifier,
       content Content,
       content-identifier ContentIdentifier OPTIONAL,
       message-security-label MessageSecurityLabel OPTIONAL } }

MessageOriginAuthenticationAlgorithmIdentifier ::= AlgorithmIdentifier

message-security-label EXTENSION ::= {
       MessageSecurityLabel,
       RECOMMENDED CRITICALITY {for-delivery},
       IDENTIFIED BY standard-extension:20 }

MessageSecurityLabel ::= SecurityLabel

proof-of-submission-request EXTENSION ::= {
       ProofOfSubmissionRequest IF ABSENT proof-of-submission-not-requested,
       RECOMMENDED CRITICALITY {for-submission},
       IDENTIFIED BY standard-extension:21 }

ProofOfSubmissionRequest ::= ENUMERATED {
       proof-of-submission-not-requested (0),
       proof-of-submission-requested (1) }

proof-of-delivery-request EXTENSION ::= {
       ProofOfDeliveryRequest IF ABSENT proof-of-delivery-not-requested,
       RECOMMENDED CRITICALITY {for-delivery},
       IDENTIFIED BY standard-extension:22 }

ProofOfDeliveryRequest ::= ENUMERATED {
       proof-of-delivery-not-requested (0),
       proof-of-delivery-requested (1) }

content-correlator EXTENSION ::= {
       ContentCorrelator,
       IDENTIFIED BY standard-extension:23 }

ContentCorrelator ::= CHOICE {
       ia5text IA5String,
       octets  OCTET STRING }

probe-origin-authentication-check EXTENSION ::= {
       ProbeOriginAuthenticationCheck,
       RECOMMENDED CRITICALITY {for-delivery},
       IDENTIFIED BY standard-extension:24 }
```

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

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

```
--      Figure 2 - Part 21 of 29

ProbeOriginAuthenticationCheck ::= SIGNATURE { SEQUENCE {
       algorithm-identifier ProbeOriginAuthenticationAlgorithmIdentifier,
       content-identifier ContentIdentifier OPTIONAL,
       message-security-label MessageSecurityLabel OPTIONAL } }

ProbeOriginAuthenticationAlgorithmIdentifier ::= AlgorithmIdentifier

redirection-history EXTENSION ::= {
       RedirectionHistory,
       IDENTIFIED BY standard-extension:25 }

RedirectionHistory ::= SEQUENCE SIZE (1..ub-redirections) OF Redirection

Redirection ::= SEQUENCE {
       intended-recipient-name IntendedRecipientName,
       redirection-reason RedirectionReason }

IntendedRecipientName ::= SEQUENCE {
       intended-recipient ORAddressAndOptionalDirectoryName,
       redirection-time Time }

RedirectionReason ::= ENUMERATED {
       recipient-assigned-alternate-recipient (0),
       originator-requested-alternate-recipient (1),
       recipient-MD-assigned-alternate-recipient (2),
       -- The following values may not be supported by implementations of earlier versions of this Service Definition
       directory-look-up (3),
       alias (4),
       ... }

dl-expansion-history EXTENSION ::= {
       DLExpansionHistory,
       IDENTIFIED BY standard-extension:26 }

DLExpansionHistory ::= SEQUENCE SIZE (1..ub-dl-expansions) OF DLExpansion

DLExpansion ::= SEQUENCE {
       dl ORAddressAndOptionalDirectoryName,
       dl-expansion-time Time }

physical-forwarding-address EXTENSION ::= {
       PhysicalForwardingAddress,
       IDENTIFIED BY standard-extension:27 }

PhysicalForwardingAddress ::= ORAddressAndOptionalDirectoryName

recipient-certificate EXTENSION ::= {
       RecipientCertificate,
       IDENTIFIED BY standard-extension:28 }

proof-of-delivery EXTENSION ::= {
       ProofOfDelivery,
       IDENTIFIED BY standard-extension:29 }

originator-and-DL-expansion-history EXTENSION ::= {
       OriginatorAndDLExpansionHistory,
       IDENTIFIED BY standard-extension:30 }

OriginatorAndDLExpansionHistory ::= SEQUENCE SIZE (2..ub-orig-and-dl-expansions) OF
              OriginatorAndDLExpansion

OriginatorAndDLExpansion ::= SEQUENCE {
       originator-or-dl-name ORAddressAndOptionalDirectoryName,
       origination-or-expansion-time Time }
```


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

```
--      Figure 2 - Part 22 of 29

reporting-DL-name EXTENSION ::= {
       ReportingDLName,
       IDENTIFIED BY standard-extension:31 }

ReportingDLName ::= ORAddressAndOptionalDirectoryName

reporting-MTA-certificate EXTENSION ::= {
       ReportingMTACertificate,
       RECOMMENDED CRITICALITY {for-delivery},
       IDENTIFIED BY standard-extension:32 }

ReportingMTACertificate ::= Certificates

report-origin-authentication-check EXTENSION ::= {
       ReportOriginAuthenticationCheck,
       RECOMMENDED CRITICALITY {for-delivery},
       IDENTIFIED BY standard-extension:33 }

ReportOriginAuthenticationCheck ::= SIGNATURE { SEQUENCE {
       algorithm-identifier ReportOriginAuthenticationAlgorithmIdentifier,
       content-identifier ContentIdentifier OPTIONAL,
       message-security-label MessageSecurityLabel OPTIONAL,
       per-recipient SEQUENCE SIZE (1..ub-recipients) OF PerRecipientReportFields } }

ReportOriginAuthenticationAlgorithmIdentifier ::= AlgorithmIdentifier

PerRecipientReportFields ::= SEQUENCE {
       actual-recipient-name ActualRecipientName,
       originally-intended-recipient-name OriginallyIntendedRecipientName OPTIONAL,
       report-type CHOICE {
              delivery [0] PerRecipientDeliveryReportFields,
              non-delivery [1] PerRecipientNonDeliveryReportFields } }

PerRecipientDeliveryReportFields ::= SEQUENCE {
       message-delivery-time MessageDeliveryTime,
       type-of-MTS-user TypeOfMTSUser,
       recipient-certificate [0] RecipientCertificate OPTIONAL,
       proof-of-delivery [1] ProofOfDelivery OPTIONAL }

PerRecipientNonDeliveryReportFields ::= SEQUENCE {
       non-delivery-reason-code NonDeliveryReasonCode,
       non-delivery-diagnostic-code NonDeliveryDiagnosticCode OPTIONAL }

originating-MTA-certificate EXTENSION ::= {
       OriginatingMTACertificate,
       IDENTIFIED BY standard-extension:34 }

OriginatingMTACertificate ::= Certificates

proof-of-submission EXTENSION ::= {
       ProofOfSubmission,
       IDENTIFIED BY standard-extension:35 }

ProofOfSubmission ::= SIGNATURE { SEQUENCE {
       algorithm-identifier ProofOfSubmissionAlgorithmIdentifier,
       message-submission-envelope MessageSubmissionEnvelope,
       content Content,
       message-submission-identifier MessageSubmissionIdentifier,
       message-submission-time MessageSubmissionTime } }

ProofOfSubmissionAlgorithmIdentifier ::= AlgorithmIdentifier

reporting-MTA-name EXTENSION ::= {
       ReportingMTAName,
       IDENTIFIED BY standard-extension:39 }

ReportingMTAName ::= SEQUENCE {
       domain GlobalDomainIdentifier,
       mta-name MTAName,
       mta-directory-name [0] Name OPTIONAL }
```

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

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

```
--      Figure 2 - Part 22 of 29

multiple-originator-certificates EXTENSION ::= {
       ExtendedCertificates,
       IDENTIFIED BY standard-extension:40 }

ExtendedCertificates ::= SET SIZE (1..ub-certificates) OF ExtendedCertificate

ExtendedCertificate ::= CHOICE {
       directory-entry [0] Name,   -- Name of a Directory entry where the certificate can be found
       certificate [1] Certificates}

dl-exempted-recipients EXTENSION ::= {
       DLExemptedRecipients,
       IDENTIFIED BY standard-extension:42 }

DLExemptedRecipients ::= SET OF ORAddressAndOrDirectoryName

certificate-selectors EXTENSION ::= {
       CertificateSelectors,
       IDENTIFIED BY standard-extension:45 }

CertificateSelectors ::= SET {
       encryption-recipient           [0] CertificateAssertion OPTIONAL,
       encryption-originator          [1] CertificateAssertion OPTIONAL,
       content-integrity-check        [2] CertificateAssertion OPTIONAL,
       token-signature                [3] CertificateAssertion OPTIONAL,
       message-origin-authentication  [4] CertificateAssertion OPTIONAL}

certificate-selectors-override EXTENSION ::= {
       CertificateSelectors (WITH COMPONENTS{...,
              message-origin-authentication ABSENT}),
       IDENTIFIED BY standard-extension:46 }

-- Some standard-extensions are defined elsewhere:
--       36 (forwarding-request) in ITU-T Rec. X.413 | ISO/IEC 10021-5;
--       37 (trace-information), and 38 (internal-trace-information) in Figure 4;
--       41 (blind-copy-recipients), 43 (body-part-encryption-token), and 44 (forwarded-content-token) in
--              ITU-T Rec. X.420 | ISO/IEC 10021-7
```


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

```
--      Figure 2 - Part 23 of 29

--      Common Parameter Types

Content ::= OCTET STRING            -- when the content-type has the integer value external, the value of the
                                    -- content octet string is the ASN.1 encoding of the external-content;
                                    -- an external-content is a data type EXTERNAL

MTSIdentifier ::= [APPLICATION 4] SEQUENCE {
       global-domain-identifier GlobalDomainIdentifier,
       local-identifier LocalIdentifier }

LocalIdentifier ::= IA5String (SIZE (1..ub-local-id-length))

GlobalDomainIdentifier ::= [APPLICATION 3] SEQUENCE {
       country-name CountryName,
       administration-domain-name AdministrationDomainName,
       private-domain-identifier PrivateDomainIdentifier OPTIONAL }

PrivateDomainIdentifier ::= CHOICE {
       numeric NumericString (SIZE (1..ub-domain-name-length)),
       printable PrintableString (SIZE (1..ub-domain-name-length)) }

MTAName ::= IA5String (SIZE (1..ub-mta-name-length))

Time ::= UTCTime

--      OR Names

ORAddressAndOrDirectoryName ::= ORName

ORAddressAndOptionalDirectoryName ::= ORName

ORName ::= [APPLICATION 0] SEQUENCE {
       -- address -- COMPONENTS OF ORAddress,
       directory-name [0] Name OPTIONAL }

ORAddress ::= SEQUENCE {
       built-in-standard-attributes BuiltInStandardAttributes,
       built-in-domain-defined-attributes BuiltInDomainDefinedAttributes OPTIONAL,
       -- see also teletex-domain-defined-attributes
       extension-attributes ExtensionAttributes OPTIONAL }

--      The OR-address is semantically absent from the OR-name if the built-in-standard-attribute
--      sequence is empty and the built-in-domain-defined-attributes and extension-attributes are both omitted.

--      Built-in Standard Attributes

BuiltInStandardAttributes ::= SEQUENCE {
       country-name CountryName OPTIONAL,
       administration-domain-name AdministrationDomainName OPTIONAL,
       network-address [0] NetworkAddress OPTIONAL,
       -- see also extended-network-address
       terminal-identifier [1] TerminalIdentifier OPTIONAL,
       private-domain-name [2] PrivateDomainName OPTIONAL,
       organization-name [3] OrganizationName OPTIONAL,
       -- see also teletex-organization-name
       numeric-user-identifier [4] NumericUserIdentifier OPTIONAL,
       personal-name [5] PersonalName OPTIONAL,
       -- see also teletex-personal-name
       organizational-unit-names [6] OrganizationalUnitNames OPTIONAL
       -- see also teletex-organizational-unit-names -- }
```


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

```
--      Figure 2 - Part 24 of 29

CountryName ::= [APPLICATION 1] CHOICE {
       x121-dcc-code NumericString (SIZE (ub-country-name-numeric-length)),
       iso-3166-alpha2-code PrintableString (SIZE (ub-country-name-alpha-length)) }

AdministrationDomainName ::= [APPLICATION 2] CHOICE {
       numeric NumericString (SIZE (0..ub-domain-name-length)),
       printable PrintableString (SIZE (0..ub-domain-name-length)) }

NetworkAddress ::= X121Address
-- see also extended-network-address

X121Address ::= NumericString (SIZE (1..ub-x121-address-length))

TerminalIdentifier ::= PrintableString (SIZE (1..ub-terminal-id-length))

PrivateDomainName ::= CHOICE {
       numeric NumericString (SIZE (1..ub-domain-name-length)),
       printable PrintableString (SIZE (1..ub-domain-name-length)) }

OrganizationName ::= PrintableString (SIZE (1..ub-organization-name-length))
-- see also teletex-organization-name

NumericUserIdentifier ::= NumericString (SIZE (1..ub-numeric-user-id-length))

PersonalName ::= SET {
       surname [0] PrintableString (SIZE (1..ub-surname-length)),
       given-name [1] PrintableString (SIZE (1..ub-given-name-length)) OPTIONAL,
       initials [2] PrintableString (SIZE (1..ub-initials-length)) OPTIONAL,
       generation-qualifier [3] PrintableString (SIZE (1..ub-generation-qualifier-length))
                                                                        OPTIONAL}
-- see also teletex-personal-name

OrganizationalUnitNames ::= SEQUENCE SIZE (1..ub-organizational-units) OF
                                                          OrganizationalUnitName
-- see also teletex-organizational-unit-names

OrganizationalUnitName ::= PrintableString (SIZE (1..ub-organizational-unit-name-length))

--      Built-in Domain-defined Attributes

BuiltInDomainDefinedAttributes ::= SEQUENCE SIZE (1..ub-domain-defined-attributes) OF
                                    BuiltInDomainDefinedAttribute

BuiltInDomainDefinedAttribute ::= SEQUENCE {
       type PrintableString (SIZE (1..ub-domain-defined-attribute-type-length)),
       value PrintableString (SIZE (1..ub-domain-defined-attribute-value-length)) }

--      Extension Attributes

ExtensionAttributes ::= SET SIZE (1..ub-extension-attributes) OF ExtensionAttribute

ExtensionAttribute ::= SEQUENCE {
       extension-attribute-type [0] EXTENSION-ATTRIBUTE.&id ({ExtensionAttributeTable}),
       extension-attribute-value [1] EXTENSION-ATTRIBUTE.&Type ({ExtensionAttributeTable}
                                                        {@extension-attribute-type}) }

EXTENSION-ATTRIBUTE ::= CLASS {
       &id    INTEGER (0..ub-extension-attributes) UNIQUE,
       &Type }
WITH SYNTAX {&Type IDENTIFIED BY &id}
```


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

```
--      Figure 2 - Part 25 of 29

ExtensionAttributeTable EXTENSION-ATTRIBUTE ::= {
       common-name |
       teletex-common-name |
       universal-common-name |
       teletex-organization-name |
       universal-organization-name |
       teletex-personal-name |
       universal-personal-name |
       teletex-organizational-unit-names |
       universal-organizational-unit-names |
       teletex-domain-defined-attributes |
       universal-domain-defined-attributes |
       pds-name |
       physical-delivery-country-name |
       postal-code |
       physical-delivery-office-name |
       universal-physical-delivery-office-name |
       physical-delivery-office-number |
       universal-physical-delivery-office-number |
       extension-OR-address-components |
       universal-extension-OR-address-components |
       physical-delivery-personal-name |
       universal-physical-delivery-personal-name |
       physical-delivery-organization-name |
       universal-physical-delivery-organization-name |
       extension-physical-delivery-address-components |
       universal-extension-physical-delivery-address-components |
       unformatted-postal-address |
       universal-unformatted-postal-address |
       street-address |
       universal-street-address |
       post-office-box-address |
       universal-post-office-box-address |
       poste-restante-address |
       universal-poste-restante-address |
       unique-postal-name |
       universal-unique-postal-name |
       local-postal-attributes |
       universal-local-postal-attributes |
       extended-network-address |
       terminal-type }

--      Extension Standard Attributes

common-name EXTENSION-ATTRIBUTE ::= {CommonName IDENTIFIED BY 1}

CommonName ::= PrintableString (SIZE (1..ub-common-name-length))

teletex-common-name EXTENSION-ATTRIBUTE ::= {TeletexCommonName IDENTIFIED BY 2}

TeletexCommonName ::= TeletexString (SIZE (1..ub-common-name-length))

universal-common-name EXTENSION-ATTRIBUTE ::= {UniversalCommonName IDENTIFIED BY 24}

UniversalCommonName ::= UniversalOrBMPString {ub-common-name-length}

teletex-organization-name EXTENSION-ATTRIBUTE ::= {TeletexOrganizationName IDENTIFIED BY 3}

TeletexOrganizationName ::= TeletexString (SIZE (1..ub-organization-name-length))

universal-organization-name EXTENSION-ATTRIBUTE ::=
       {UniversalOrganizationName IDENTIFIED BY 25}

UniversalOrganizationName ::= UniversalOrBMPString {ub-organization-name-length}

teletex-personal-name EXTENSION-ATTRIBUTE ::= {TeletexPersonalName IDENTIFIED BY 4}

TeletexPersonalName ::= SET {
       surname [0] TeletexString (SIZE (1..ub-surname-length)),
       given-name [1] TeletexString (SIZE (1..ub-given-name-length)) OPTIONAL,
       initials [2] TeletexString (SIZE (1..ub-initials-length)) OPTIONAL,
       generation-qualifier [3] TeletexString (SIZE (1..ub-generation-qualifier-length))
                                                                              OPTIONAL }
```


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

```
--      Figure 2 - Part 25 of 29

universal-personal-name EXTENSION-ATTRIBUTE ::= {UniversalPersonalName IDENTIFIED BY 26}

UniversalPersonalName ::= SET {
       surname [0] UniversalOrBMPString {ub-universal-surname-length},
       --      If a language is specified within surname, then that language applies to each of the following
       --      optional components unless the component specifies another language.
       given-name [1] UniversalOrBMPString {ub-universal-given-name-length} OPTIONAL,
       initials [2] UniversalOrBMPString {ub-universal-initials-length} OPTIONAL,
       generation-qualifier [3]
              UniversalOrBMPString {ub-universal-generation-qualifier-length} OPTIONAL }

teletex-organizational-unit-names EXTENSION-ATTRIBUTE ::=
       {TeletexOrganizationalUnitNames IDENTIFIED BY 5}

TeletexOrganizationalUnitNames ::= SEQUENCE SIZE (1..ub-organizational-units) OF
       TeletexOrganizationalUnitName

TeletexOrganizationalUnitName ::= TeletexString (SIZE (1..ub-organizational-unit-name-length))

universal-organizational-unit-names EXTENSION-ATTRIBUTE ::=
       {UniversalOrganizationalUnitNames IDENTIFIED BY 27}

UniversalOrganizationalUnitNames ::= SEQUENCE SIZE (1..ub-organizational-units) OF
       UniversalOrganizationalUnitName
       --      If a unit name specifies a language, then that language applies to subordinate unit names unless
       --      the subordinate specifies another language.

UniversalOrganizationalUnitName ::= UniversalOrBMPString {ub-organizational-unit-name-length}

UniversalOrBMPString{INTEGER:ub-string-length} ::= SET {
       character-encoding CHOICE {
              two-octets BMPString (SIZE(1..ub-string-length)),
              four-octets UniversalString (SIZE(1..ub-string-length)) },
       iso-639-language-code PrintableString (SIZE(2|5)) OPTIONAL }

pds-name EXTENSION-ATTRIBUTE ::= {PDSName IDENTIFIED BY 7}

PDSName ::= PrintableString (SIZE (1..ub-pds-name-length))

physical-delivery-country-name EXTENSION-ATTRIBUTE ::=
       {PhysicalDeliveryCountryName IDENTIFIED BY 8}
```


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

```
--      Figure 2 - Part 26 of 29

PhysicalDeliveryCountryName ::= CHOICE {
       x121-dcc-code NumericString (SIZE (ub-country-name-numeric-length)),
       iso-3166-alpha2-code PrintableString (SIZE (ub-country-name-alpha-length)) }

postal-code EXTENSION-ATTRIBUTE ::= {PostalCode IDENTIFIED BY 9}

PostalCode ::= CHOICE {
       numeric-code NumericString (SIZE (1..ub-postal-code-length)),
       printable-code PrintableString (SIZE (1..ub-postal-code-length)) }

physical-delivery-office-name EXTENSION-ATTRIBUTE ::=
       {PhysicalDeliveryOfficeName IDENTIFIED BY 10}

PhysicalDeliveryOfficeName ::= PDSParameter

universal-physical-delivery-office-name EXTENSION-ATTRIBUTE ::=
       {UniversalPhysicalDeliveryOfficeName IDENTIFIED BY 29}

UniversalPhysicalDeliveryOfficeName ::= UniversalPDSParameter

physical-delivery-office-number EXTENSION-ATTRIBUTE ::=
       {PhysicalDeliveryOfficeNumber IDENTIFIED BY 11}

PhysicalDeliveryOfficeNumber ::= PDSParameter

universal-physical-delivery-office-number EXTENSION-ATTRIBUTE ::=
       {UniversalPhysicalDeliveryOfficeNumber IDENTIFIED BY 30}

UniversalPhysicalDeliveryOfficeNumber ::= UniversalPDSParameter

extension-OR-address-components EXTENSION-ATTRIBUTE ::=
       {ExtensionORAddressComponents IDENTIFIED BY 12}

ExtensionORAddressComponents ::= PDSParameter

universal-extension-OR-address-components EXTENSION-ATTRIBUTE ::=
       {UniversalExtensionORAddressComponents IDENTIFIED BY 31}

UniversalExtensionORAddressComponents ::= UniversalPDSParameter

physical-delivery-personal-name EXTENSION-ATTRIBUTE ::=
       {PhysicalDeliveryPersonalName IDENTIFIED BY 13}

PhysicalDeliveryPersonalName ::= PDSParameter

universal-physical-delivery-personal-name EXTENSION-ATTRIBUTE ::=
       {UniversalPhysicalDeliveryPersonalName IDENTIFIED BY 32}

UniversalPhysicalDeliveryPersonalName ::= UniversalPDSParameter

physical-delivery-organization-name EXTENSION-ATTRIBUTE ::=
       {PhysicalDeliveryOrganizationName IDENTIFIED BY 14}

PhysicalDeliveryOrganizationName ::= PDSParameter

universal-physical-delivery-organization-name EXTENSION-ATTRIBUTE ::=
       {UniversalPhysicalDeliveryOrganizationName IDENTIFIED BY 33}

UniversalPhysicalDeliveryOrganizationName ::= UniversalPDSParameter

extension-physical-delivery-address-components EXTENSION-ATTRIBUTE ::=
       {ExtensionPhysicalDeliveryAddressComponents IDENTIFIED BY 15}

ExtensionPhysicalDeliveryAddressComponents ::= PDSParameter

universal-extension-physical-delivery-address-components EXTENSION-ATTRIBUTE ::=
       {UniversalExtensionPhysicalDeliveryAddressComponents IDENTIFIED BY 34}

UniversalExtensionPhysicalDeliveryAddressComponents ::= UniversalPDSParameter
```


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

```
--      Figure 2 - Part 26 of 29

unformatted-postal-address EXTENSION-ATTRIBUTE ::=
       {UnformattedPostalAddress IDENTIFIED BY 16}

UnformattedPostalAddress ::= SET {
       printable-address SEQUENCE SIZE (1..ub-pds-physical-address-lines) OF
              PrintableString (SIZE (1..ub-pds-parameter-length)) OPTIONAL,
       teletex-string TeletexString (SIZE (1..ub-unformatted-address-length)) OPTIONAL }

universal-unformatted-postal-address EXTENSION-ATTRIBUTE ::=
       {UniversalUnformattedPostalAddress IDENTIFIED BY 35}

UniversalUnformattedPostalAddress ::= UniversalOrBMPString {ub-unformatted-address-length}

street-address EXTENSION-ATTRIBUTE ::= {StreetAddress IDENTIFIED BY 17}

StreetAddress ::= PDSParameter

universal-street-address EXTENSION-ATTRIBUTE ::= {UniversalStreetAddress IDENTIFIED BY 36}

UniversalStreetAddress ::= UniversalPDSParameter

post-office-box-address EXTENSION-ATTRIBUTE ::= {PostOfficeBoxAddress IDENTIFIED BY 18}

PostOfficeBoxAddress ::= PDSParameter

universal-post-office-box-address EXTENSION-ATTRIBUTE ::=
       {UniversalPostOfficeBoxAddress IDENTIFIED BY 37}

UniversalPostOfficeBoxAddress ::= UniversalPDSParameter

poste-restante-address EXTENSION-ATTRIBUTE ::= {PosteRestanteAddress IDENTIFIED BY 19}

PosteRestanteAddress ::= PDSParameter

universal-poste-restante-address EXTENSION-ATTRIBUTE ::=
       {UniversalPosteRestanteAddress IDENTIFIED BY 38}

UniversalPosteRestanteAddress ::= UniversalPDSParameter

unique-postal-name EXTENSION-ATTRIBUTE ::= {UniquePostalName IDENTIFIED BY 20}

UniquePostalName ::= PDSParameter

universal-unique-postal-name EXTENSION-ATTRIBUTE ::=
       {UniversalUniquePostalName IDENTIFIED BY 39}

UniversalUniquePostalName ::= UniversalPDSParameter

local-postal-attributes EXTENSION-ATTRIBUTE ::= {LocalPostalAttributes IDENTIFIED BY 21}

LocalPostalAttributes ::= PDSParameter
```

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

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

```
--      Figure 2 - Part 27 of 29

universal-local-postal-attributes EXTENSION-ATTRIBUTE ::=
       {UniversalLocalPostalAttributes IDENTIFIED BY 40}

UniversalLocalPostalAttributes ::= UniversalPDSParameter

PDSParameter ::= SET {
       printable-string PrintableString (SIZE(1..ub-pds-parameter-length)) OPTIONAL,
       teletex-string TeletexString (SIZE(1..ub-pds-parameter-length)) OPTIONAL }

UniversalPDSParameter ::= UniversalOrBMPString {ub-pds-parameter-length}

extended-network-address EXTENSION-ATTRIBUTE ::= {ExtendedNetworkAddress IDENTIFIED BY 22}

ExtendedNetworkAddress ::= CHOICE {
       e163-4-address SEQUENCE {
              number [0] NumericString (SIZE (1..ub-e163-4-number-length)),
              sub-address [1] NumericString (SIZE (1..ub-e163-4-sub-address-length))
                                                                          OPTIONAL },
       psap-address [0] PresentationAddress }

terminal-type EXTENSION-ATTRIBUTE ::= {TerminalType IDENTIFIED BY 23}

TerminalType ::= INTEGER {
       telex (3),
       teletex (4),
       g3-facsimile (5),
       g4-facsimile (6),
       ia5-terminal (7),
       videotex (8) } (0..ub-integer-options)

--      Extension Domain-defined Attributes

teletex-domain-defined-attributes EXTENSION-ATTRIBUTE ::=
       {TeletexDomainDefinedAttributes IDENTIFIED BY 6}

TeletexDomainDefinedAttributes ::= SEQUENCE SIZE (1..ub-domain-defined-attributes) OF
       TeletexDomainDefinedAttribute

TeletexDomainDefinedAttribute ::= SEQUENCE {
       type TeletexString (SIZE (1..ub-domain-defined-attribute-type-length)),
       value TeletexString (SIZE (1..ub-domain-defined-attribute-value-length)) }

universal-domain-defined-attributes EXTENSION-ATTRIBUTE ::=
       {UniversalDomainDefinedAttributes IDENTIFIED BY 28}

UniversalDomainDefinedAttributes ::= SEQUENCE SIZE (1..ub-domain-defined-attributes) OF
       UniversalDomainDefinedAttribute

UniversalDomainDefinedAttribute ::= SEQUENCE {
       type UniversalOrBMPString {ub-domain-defined-attribute-type-length},
       value UniversalOrBMPString {ub-domain-defined-attribute-value-length} }

--      Encoded Information Types

EncodedInformationTypes ::= [APPLICATION 5] SET {
       built-in-encoded-information-types [0] BuiltInEncodedInformationTypes,
       -- non-basic-parameters -- COMPONENTS OF NonBasicParameters,
       extended-encoded-information-types [4] ExtendedEncodedInformationTypes OPTIONAL }

--      Built-in Encoded Information Types

BuiltInEncodedInformationTypes ::= BIT STRING {
       unknown (0),
       ia5-text (2),
       g3-facsimile (3),
       g4-class-1 (4),
       teletex (5),
       videotex (6),
       voice (7),
       sfd (8),
       mixed-mode (9) } (SIZE (0..ub-built-in-encoded-information-types))
```


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

```
--      Figure 2 - Part 27 of 29

--      Extended Encoded Information Types

ExtendedEncodedInformationTypes ::= SET SIZE (1..ub-encoded-information-types) OF
              ExtendedEncodedInformationType

ExtendedEncodedInformationType ::= OBJECT IDENTIFIER

--      Non-basic Parameters

NonBasicParameters ::= SET {
       g3-facsimile [1] G3FacsimileNonBasicParameters DEFAULT { },
       teletex [2] TeletexNonBasicParameters DEFAULT { } }
```


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

```
--      Figure 2 - Part 28 of 29

G3FacsimileNonBasicParameters ::= BIT STRING {
       two-dimensional (8),                -- As defined in ITU-T Recommendation T.30
       fine-resolution (9),                --
       unlimited-length (20),              -- These bit values are chosen such that when
       b4-length (21),                     -- encoded using ASN.1 Basic Encoding Rules
       a3-width (22),                      -- the resulting octets have the same values
       b4-width (23),                      -- as for T.30 encoding
       t6-coding (25),                     --
       uncompressed (30),                  -- Trailing zero bits are not significant.
       width-middle-864-of-1728 (37),      -- It is recommended that implementations
       width-middle-1216-of-1728 (38),     -- should not encode more than 32 bits unless
       resolution-type (44),               -- higher numbered bits are non-zero.
       resolution-400x400 (45),
       resolution-300x300 (46),
       resolution-8x15 (47),
       edi (49),
       dtm (50),
       bft (51),
       mixed-mode (58),
       character-mode (60),
       twelve-bits (65),
       preferred-huffmann (66),
       full-colour (67),
       jpeg (68),
       processable-mode-26 (71) }

TeletexNonBasicParameters ::= SET {
       graphic-character-sets [0] TeletexString OPTIONAL,
       control-character-sets [1] TeletexString OPTIONAL,
       page-formats [2] OCTET STRING OPTIONAL,
       miscellaneous-terminal-capabilities [3] TeletexString OPTIONAL,
       private-use [4] OCTET STRING OPTIONAL      -- maximum ub-teletex-private-use-length octets -- }
       -- as defined in CCITT Recommendation T.62

--      Token

Token ::= SEQUENCE {
       token-type-identifier [0] TOKEN.&id ({TokensTable}),
       token [1] TOKEN.&Type ({TokensTable} {@token-type-identifier}) }

TOKEN ::= TYPE-IDENTIFIER

TokensTable TOKEN ::= { asymmetric-token, ... }

asymmetric-token TOKEN ::= {AsymmetricToken IDENTIFIED BY id-tok-asymmetricToken}

AsymmetricToken ::= SIGNED { SEQUENCE {
       signature-algorithm-identifier AlgorithmIdentifier,
       name CHOICE {
              recipient-name RecipientName,
              mta [3] SEQUENCE {
                     global-domain-identifier GlobalDomainIdentifier OPTIONAL,
                     mta-name MTAName } },
       time Time,
       signed-data [0] TokenData OPTIONAL,
       encryption-algorithm-identifier [1] AlgorithmIdentifier OPTIONAL,
       encrypted-data [2] ENCRYPTED { TokenData } OPTIONAL } }

TokenData ::= SEQUENCE {
       type [0] TOKEN-DATA.&id ({TokenDataTable}),
       value [1] TOKEN-DATA.&Type ({TokenDataTable} {@type}) }

TOKEN-DATA ::= CLASS {
       &id INTEGER UNIQUE,
       &Type }
WITH SYNTAX {&Type IDENTIFIED BY &id}
```


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

```
--      Figure 2 - Part 29 of 29

TokenDataTable TOKEN-DATA ::= {
       bind-token-signed-data |
       message-token-signed-data |
       message-token-encrypted-data |
       bind-token-encrypted-data, ... }

bind-token-signed-data TOKEN-DATA ::= {BindTokenSignedData IDENTIFIED BY 1}

BindTokenSignedData ::= RandomNumber

RandomNumber ::= BIT STRING

message-token-signed-data TOKEN-DATA ::= {MessageTokenSignedData IDENTIFIED BY 2}

MessageTokenSignedData ::= SEQUENCE {
       content-confidentiality-algorithm-identifier [0]
              ContentConfidentialityAlgorithmIdentifier OPTIONAL,
       content-integrity-check [1] ContentIntegrityCheck OPTIONAL,
       message-security-label [2] MessageSecurityLabel OPTIONAL,
       proof-of-delivery-request [3] ProofOfDeliveryRequest OPTIONAL,
       message-sequence-number [4] INTEGER OPTIONAL }

message-token-encrypted-data TOKEN-DATA ::= {MessageTokenEncryptedData IDENTIFIED BY 3}

MessageTokenEncryptedData ::= SEQUENCE {
       content-confidentiality-key [0] EncryptionKey OPTIONAL,
       content-integrity-check [1] ContentIntegrityCheck OPTIONAL,
       message-security-label [2] MessageSecurityLabel OPTIONAL,
       content-integrity-key [3] EncryptionKey OPTIONAL,
       message-sequence-number [4] INTEGER OPTIONAL }

EncryptionKey ::= BIT STRING

bind-token-encrypted-data TOKEN-DATA ::= {BindTokenEncryptedData IDENTIFIED BY 4}

BindTokenEncryptedData ::= EXTERNAL

--      Security Label

SecurityLabel ::= SET {
       security-policy-identifier SecurityPolicyIdentifier OPTIONAL,
       security-classification SecurityClassification OPTIONAL,
       privacy-mark PrivacyMark OPTIONAL,
       security-categories SecurityCategories OPTIONAL }

SecurityPolicyIdentifier ::= OBJECT IDENTIFIER

SecurityClassification ::= INTEGER {
       unmarked (0),
       unclassified (1),
       restricted (2),
       confidential (3),
       secret (4),
       top-secret (5) } (0..ub-integer-options)

PrivacyMark ::= PrintableString (SIZE (1..ub-privacy-mark-length))

SecurityCategories ::= SET SIZE (1..ub-security-categories) OF SecurityCategory

SecurityCategory ::= SEQUENCE {
       type [0] SECURITY-CATEGORY.&id ({SecurityCategoriesTable}),
       value [1] SECURITY-CATEGORY.&Type ({SecurityCategoriesTable} {@type}) }

SECURITY-CATEGORY ::= TYPE-IDENTIFIER

SecurityCategoriesTable SECURITY-CATEGORY ::= { ... }

END     -- of MTSAbstractService
```

Figure 2 – Abstract Syntax Definition of the MTS Abstract Service (end)

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

SECTION THREE – MESSAGE TRANSFER AGENT ABSTRACT SERVICE

10 Refined Message Transfer System Model

Clause 6 describes the MTS as an object, without reference to its internal structure. This clause refines the MTS model, and exposes its component objects and the ports shared between them.

Figure 3 models the MTS and reveals its internal structure.

The MTS comprises a collection of message-transfer-agent (MTA) objects, which cooperate together to form the MTS and offer the MTS Abstract Service to its users. It is the MTAs which perform the active functions of the MTS, i.e., transfer of messages, probes and reports, generation of reports, and content conversion.

MTA objects also have ports, some of which are precisely those which are also visible at the boundary of the MTS object, i.e., submission-ports, delivery-ports and administration-ports. However, MTAs also have another type of port – a transfer-port – which are concerned with the distribution of the MTS Abstract Service between the MTAs, and are not visible at the boundary of the MTS object.

A transfer-port enables an MTA to transfer messages, probes and reports to another MTA. In general, a message, probe or report may have to be transferred a number of times between different MTAs to reach its intended destination.

If a message is addressed to multiple recipients served by several different MTAs, the message must be transferred through the MTS along several different paths. From the perspective of an MTA transferring such a message, some recipients may be reached via one path while other recipients may be reached via another. At such an MTA, two copies of the message are created, and each is transferred to the next MTA along its respective path. The copying and branching of the message is repeated until each copy has reached a final destination MTA, where the message can be delivered to one or more recipient MTS-users.

Every MTA along a path taken by a message is responsible for delivering or transferring the message to a particular subset of the originally-specified-recipients. Other MTAs take care of the delivery or transfer to remaining recipients, using copies of the messages created along the way.

Reports on the delivery or non-delivery of a message to one or more recipient MTS-users, are generated by MTAs in accordance with the request of the originator of the message and the originating-MTA. An MTA may generate a delivery-report upon successfully delivering a copy of a message to a recipient MTS-user. It may generate a non-delivery-report upon determining that a copy of a message is undeliverable to one or more recipients, that is, it is unable to deliver the message to the recipient MTS-users, or it is unable to transfer the message to an adjacent MTA that would take responsibility for delivery or transferring the message further.

For efficiency, an MTA may generate a single, combined report that applies to several copies of a single, multiple recipient message for which it is responsible. Both delivery- and non-delivery-reports may be combined together. However, in order for reports to be combined in this manner, the same content conversion, if any, must have been performed on the message for all recipients to whom the report refers.

Reports that pertain to copies of the same multiple recipient message but that were generated by different MTAs are not combined by any intermediate MTAs, but instead remain distinct.

When required, an MTA may perform content conversion. When neither the originating nor the recipient MTS-user requests nor prohibits conversion, implicit conversion of a message's encoded-information-types may be performed by an MTA to suit the encoded-information-types that the recipient MTS-user is able to receive. The originating MTS-user may also explicitly request conversion of specific encoded-information-types for a particular recipient MTS-user.

The submission-, delivery- and administration-ports of an MTA, which are also visible at the boundary of the MTS, are defined in section two of this Service Definition. The remaining clauses in this section define the transfer-port of an MTA, and the procedures performed by MTAs to ensure the correct distributed operation of the MTS.

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

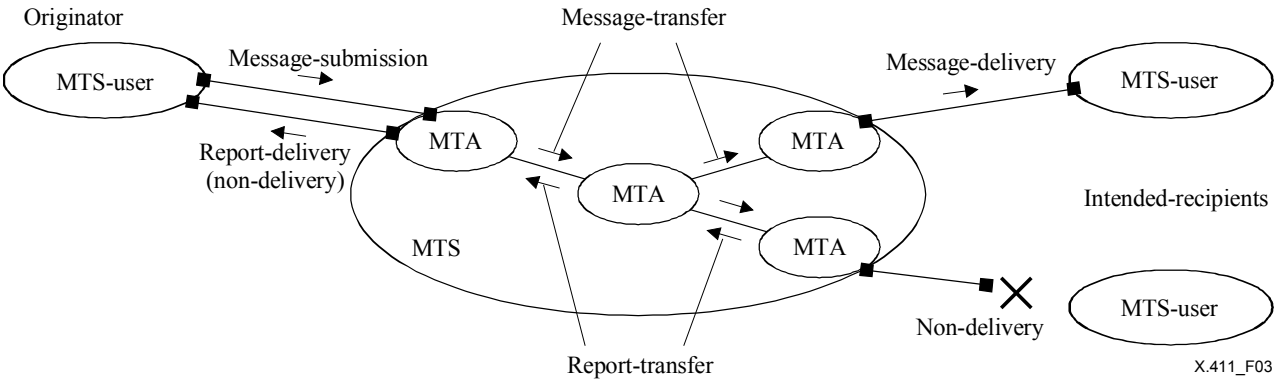


Figure 3 – Refined Message Transfer System Model

11 Message Transfer Agent Abstract Service Overview

Section two defines the MTS Abstract Service provided by the submission-, delivery- and administration-ports of an MTA. This clause defines the following abstract-operations that are provided by the transfer-ports of MTAs:

MTA-bind and MTA-unbind

a) MTA-bind

b) MTA-unbind

Transfer Port Abstract-operations

c) Message-transfer

d) Probe-transfer

e) Report-transfer.

11.1 MTA-bind and MTA-unbind

The **MTA-bind** enables an MTA to establish an association with another MTA. Abstract-operations other than MTA-bind can only be invoked in the context of an established association.

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

11.2 Transfer Port Abstract-operations

The **Message-transfer** abstract-operation enables an MTA to transfer a message to another MTA.

The **Probe-transfer** abstract-operation enables an MTA to transfer a probe to another MTA.

The **Report-transfer** abstract-operation enables an MTA to transfer a report to another MTA.

12 Message Transfer Agent Abstract Service Definition

The MTS Abstract Service is defined in clause 8. This clause defines the semantics of the parameters of the abstract-service provided by the transfer-ports of MTAs.

Clause 12.1 defines the MTA-bind and MTA-unbind. Clause 12.2 defines the transfer-port. Clause 12.3 defines some common parameter types.

The abstract-syntax of the MTA Abstract Service is defined in clause 13.

12.1 MTA-bind and MTA-unbind

This clause defines the abstract-services used to establish and release associations between MTAs.

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

12.1.1 Abstract-bind and Abstract-unbind

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

a) MTA-bind

b) MTA-unbind.

12.1.1.1 MTA-bind

The MTA-bind enables an MTA to establish an association with another MTA.

The MTA-bind establishes the **credentials** of MTAs 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 MTA-unbind).

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

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

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

12.1.1.1.1 Arguments

Table 28 lists the arguments of the MTA-bind, and for each argument qualifies its presence and indicates the clause in which the argument is defined.

Table 28 – MTA-bind Arguments

Argument	Presence	Clause
Bind Arguments		
Initiator-name	O	12.1.1.1.1.1
Initiator-credentials	O	12.1.1.1.1.2
Security-context	O	12.1.1.1.1.3

12.1.1.1.1.1 Initiator-name

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

The name is an **MTA-name**.

12.1.1.1.1.2 Initiator-credentials

This argument contains the **credentials** of the initiator of the association. It may 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 proposed, the **initiator-credentials** comprise a simple **password** associated with the **initiator-name**.

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**. 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 (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 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

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

to 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).

12.1.1.1.1.3 Security-context

This argument indicates 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 defines the sensitivity of interactions that may occur between the MTAs 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 **security-labels** associated with the MDs (MTAs).

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

12.1.1.1.2 Results

Table 29 lists the results of the MTA-bind, and for each result qualifies its presence and indicates the clause in which the result is defined.

Table 29 – MTA-bind Results

Result	Presence	Clause
Bind Results		
Responder-name	O	12.1.1.1.2.1
Responder-credentials	O	12.1.1.1.2.2

12.1.1.1.2.1 Responder-name

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

The name is an **MTA-name**.

12.1.1.1.2.2 Responder-credentials

This argument contains the **credentials** of the responder of the association. It may 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 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 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**. 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 (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 responding MTA. The **responder-certificate** may be used to convey a verified copy of the

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

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).

12.1.1.1.3 Bind-errors

The bind-errors that may disrupt the MTA-bind are defined in 12.1.2.

12.1.1.2 MTA-unbind

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

12.1.1.2.1 Arguments

The MTA-unbind service has no arguments.

12.1.1.2.2 Results

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

12.1.1.2.3 Unbind-errors

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

12.1.2 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.

12.1.2.1 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.

12.1.2.2 Busy

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

The Busy bind-error has no parameters.

12.1.2.3 Unacceptable-dialogue-mode (bind-error)

The Unacceptable-dialogue-mode bind-error reports that the dialogue-mode proposed by the initiator of the association is unacceptable to the responder (see clause 12 of ITU-T Rec. X.419 | ISO/IEC 10021-6).

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

12.1.2.4 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.

12.1.2.5 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.

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

12.2 Transfer Port

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

12.2.1 Abstract-operations

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

a) Message-transfer

b) Probe-transfer

c) Report-transfer.

12.2.1.1 Message-transfer

The Message-transfer abstract-operation enables an MTA to transfer a message to another MTA.

12.2.1.1.1 Arguments

Table 30 lists the arguments of the Message-transfer abstract-operation, and for each argument qualifies its presence and identifies the clause in which the argument is defined.

12.2.1.1.1.1 Message-identifier

This argument contains an **MTS-identifier** that distinguishes the message from all other messages, probes and reports within the MTS. It shall be generated by the originating-MTA of the message, and shall have the same value as the **message-submission-identifier** supplied to the originator of the message when the message was submitted, and the **message-delivery-identifier** supplied to the recipients of the message when the message is delivered.

When a message is copied for routing to multiple recipients via different MTAs, each copy of the message bears the **message-identifier** of the original.

12.2.1.1.1.2 Per-domain-bilateral-information

This argument contains information intended for MDs which the message will encounter as it is transferred through the MTS. It may be generated by the originating-MD of the message.

This argument may contain zero or more elements, each of which comprises:

the **bilateral-information** intended for an MD;

the **country-name** and, optionally, the **administration-domain-name** and, optionally, the **private-domain-identifier** of the MD for which the **bilateral-information** is intended.

12.2.1.1.1.3 Trace-information

This argument documents the actions taken on the message (or probe or report) by each MD through which the message (or probe or report) passes as it is transferred through the MTS (see 12.3.1). It shall be generated by each MD through which the message (or probe or report) passes.

Table 30 – Message-transfer Arguments

Argument	Presence	Clause
Relaying Arguments		
Message-identifier	M	12.2.1.1.1.1
Per-domain-bilateral-information	C	12.2.1.1.1.2
Trace-information	M	12.2.1.1.1.3
Internal-trace-information	C	12.2.1.1.1.4
DL-expansion-history	C	8.3.1.1.1.7
Originator Argument		
Originator-name	M	8.2.1.1.1.1

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

Table 30 – Message-transfer Arguments

Argument	Presence	Clause
Recipient Arguments		
Recipient-name	M	8.2.1.1.1.2
Originally-specified-recipient-number	M	12.2.1.1.1.5
Responsibility	M	12.2.1.1.1.6
DL-expansion-prohibited	C	8.2.1.1.1.6
Disclosure-of-other-recipients	C	8.2.1.1.1.7
DL-exempted-recipients	O	8.2.1.1.1.40
Redirection Arguments		
Alternate-recipient-allowed	C	8.2.1.1.1.3
Recipient-reassignment-prohibited	C	8.2.1.1.1.4
Originator-requested-alternate-recipient	C	8.2.1.1.1.5
Redirection-history	C	8.3.1.1.1.5
Priority Argument		
Priority	C	8.2.1.1.1.8
Conversion Arguments		
Implicit-conversion-prohibited	C	8.2.1.1.1.9
Conversion-with-loss-prohibited	C	8.2.1.1.1.10
Explicit-conversion	C	12.2.1.1.1.9
Delivery Time Arguments		
Deferred-delivery-time	C	12.2.1.1.1.7
Latest-delivery-time	C	8.2.1.1.1.13
Delivery Method Argument		
Requested-delivery-method	C	8.2.1.1.1.14
Physical Delivery Arguments		
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
Delivery Report Request Arguments		
Originator-report-request	M	8.2.1.1.1.22
Originating-MTA-report-request	M	12.2.1.1.1.8
Content-return-request	C	8.2.1.1.1.23
Physical-delivery-report-request	C	8.2.1.1.1.24
Security Arguments		
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

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

Table 30 – Message-transfer Arguments

Argument	Presence	Clause
Content Arguments		
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-correlator	C	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

12.2.1.1.1.4 Internal-trace-information

This argument documents the actions taken on the message (or probe or report) by each MTA through which the message (or probe or report) passes as it is transferred within an MD (see 12.3.1). It shall be generated by each MTA through which the message (or probe or report) passes within an MD.

As a matter of local policy, an MTA may (but is not required to) remove **internal-trace-information** relating to other MDs when performing delivery, or when transferring to another MD, or on receiving from another MD.

12.2.1.1.1.5 Originally-specified-recipient-number

This argument shall be generated by the originating-MTA of the message. A different value of this argument is specified for each originally-specified-recipient of the message.

The **originally-specified-recipient-number** is an integer value in the range that begins with one and ends with the number of originally-specified-recipients.

There is a one-to-one relationship between a particular **originally-specified-recipient-number** value and a particular **recipient-name** at the time of message-submission; it should not be assumed that this is a singular relationship at the time of message-delivery. That is, an **originally-specified-recipient-number** value can be used to distinguish an originally specified **recipient-name**, but not an actual recipient that will receive the message.

12.2.1.1.1.6 Responsibility

This argument indicates whether the receiving-MTA shall have the responsibility to either deliver the message to a recipient or to transfer it to another MTA for subsequent delivery to the recipient. It shall be generated by the sending-MTA. A different value of this argument may be specified for each recipient of the message.

This argument may have one of the following values: **responsible** or **not-responsible**.

12.2.1.1.1.7 Deferred-delivery-time

This argument is defined in 8.2.1.1.1.12. It may appear in a message at a transfer-port if there is a bilateral agreement that an MTA other than the originating-MTA of the message will defer the delivery of the message. It shall be absent once the request for deferral has been honoured.

In the absence of a bilateral agreement, the MTA shall, as a local matter, either:

a) defer delivery of the message, or

b) process the message as if the **deferred-delivery-time** was not present, or

c) if the deferred delivery time has not yet passed, cause the message to be non-delivered with **non-delivery-reason-code** set to **deferred-delivery-not-performed** and **non-delivery-diagnostic-code** set to **no-bilateral-agreement**.

12.2.1.1.1.8 Originating-MTA-report-request

This argument indicates the kind of report requested by the originating-MTA. It shall be generated by the originating-MTA 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:

non-delivery-report: a report is returned only in case of non-delivery, and it contains only the **last-trace-information**;

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

report: a report is returned in case of delivery or non-delivery, and it contains only the **last-trace-information**;

audited-report: a report is returned in case of delivery or non-delivery, and it contains all of the **trace-information**.

The **originating-MTA-report-request** argument shall specify at least the report level specified in the **originator-report-request** argument, where the increasing order of report levels is **no-report**, **non-delivery-report**, **report**, **audited-report**.

12.2.1.1.1.9 Explicit-conversion

This argument is defined in 8.2.1.1.1.11. Once the specified explicit conversion has been performed, the argument shall be removed.

12.2.1.1.2 Results

The Message-transfer abstract-operation does not return a result.

12.2.1.1.3 Abstract-errors

There are no abstract-errors that may disrupt the Message-transfer abstract-operation.

12.2.1.2 Probe-transfer

The Probe-transfer abstract-operation enables an MTA to transfer a probe to another MTA.

12.2.1.2.1 Arguments

Table 31 lists the arguments of the Probe-transfer abstract-operation, and for each argument qualifies its presence and identifies the clause in which the argument is defined.

12.2.1.2.1.1 Probe-identifier

This argument contains an **MTS-identifier** that distinguishes the probe from all other messages, probes and reports within the MTS. It shall be generated by the originating-MTA of the probe, and shall have the same value as the **probe-submission-identifier** supplied to the originator of the probe when the probe was submitted.

12.2.1.2.2 Results

The Probe-transfer abstract-operation does not return a result.

12.2.1.2.3 Abstract-errors

There are no abstract-errors that may disrupt the Probe-transfer abstract-operation.

12.2.1.3 Report-transfer

The Report-transfer abstract-operation enables an MTA to transfer a report to another MTA.

Table 31 – Probe-transfer Arguments

Argument	Presence	Clause
Relaying Arguments		
Probe-identifier	M	12.2.1.2.1.1
Per-domain-bilateral-information	C	12.2.1.1.1.2
Trace-information	M	12.2.1.1.1.3
Internal-trace-information	C	12.2.1.1.1.4
Originator Argument		
Originator-name	M	8.2.1.1.1.1
Recipient Arguments		
Recipient-name	M	8.2.1.1.1.2
Originally-specified-recipient-number	M	12.2.1.1.1.5
Responsibility	M	12.2.1.1.1.6
DL-expansion-prohibited	C	8.2.1.1.1.6

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

Table 31 – Probe-transfer Arguments

Argument	Presence	Clause
Redirection Arguments		
Alternate-recipient-allowed	C	8.2.1.1.1.3
Recipient-reassignment-prohibited	C	8.2.1.1.1.4
Originator-requested-alternate-recipient	C	8.2.1.1.1.5
Redirection-history	C	8.3.1.1.1.5
Conversion Arguments		
Implicit-conversion-prohibited	C	8.2.1.1.1.9
Conversion-with-loss-prohibited	C	8.2.1.1.1.10
Explicit-conversion	C	8.2.1.1.1.11
Delivery Method Argument		
Requested-delivery-method	C	8.2.1.1.1.14
Physical Delivery Argument		
Physical-rendition-attributes	C	8.2.1.1.1.20
Report Request Arguments		
Originator-report-request	M	8.2.1.1.1.22
Originating-MTA-report-request	M	12.2.1.1.1.8
Security Arguments		
Originator-certificate	C	8.2.1.1.1.25
Probe-origin-authentication-check	C	8.2.1.2.1.1
Message-security-label	C	8.2.1.1.1.30
Content Arguments		
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-correlator	C	8.2.1.1.1.36
Content-length	C	8.2.1.2.1.2
Notification-type	C	8.2.1.1.1.38
Service-message	O	8.2.1.1.1.39

12.2.1.3.1 Arguments

Table 32 lists the arguments of the Report-transfer abstract-operation, and for each argument qualifies its presence and identifies the clause in which the argument is defined.

Table 32 – Report-transfer Arguments

Argument	Presence	Clause
Relaying Arguments		
Report-identifier	M	12.2.1.3.1.1
Trace-information	M	12.2.1.1.1.3
Internal-trace-information	C	12.2.1.1.1.4
Redirection-history	C	8.3.1.2.1.5
Report Origination Argument		
Reporting-MTA-name	C	8.3.1.2.1.17
Report Destination Argument		
Report-destination-name	M	12.2.1.3.1.2
Report Request Argument		
Originator-report-request	M	8.2.1.1.1.22

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

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

Table 32 – Report-transfer Arguments

Argument	Presence	Clause
Subject Trace Arguments		
Subject-identifier	M	12.2.1.3.1.3
Originally-specified-recipient-number	M	12.2.1.1.1.5
Subject-intermediate-trace-information	C	12.2.1.3.1.4
Arrival-time	M	12.2.1.3.1.5
Originator-and-DL-expansion-history	C	8.3.1.2.1.3
Reporting-DL-name	C	8.3.1.2.1.4
Conversion Argument		
Converted-encoded-information-types	C	8.3.1.2.1.6
Supplementary Information Arguments		
Supplementary-information	C	8.3.1.2.1.7
Physical-forwarding-address	C	8.3.1.2.1.8
Subject Redirection Arguments		
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
Content Arguments		
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
Delivery Arguments		
Message-delivery-time	C	8.3.1.2.1.9
Type-of-MTS-user	C	8.3.1.2.1.10
Non-delivery Arguments		
Non-delivery-reason-code	C	8.3.1.2.1.11
Non-delivery-diagnostic-code	C	8.3.1.2.1.12
Security Arguments		
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
Additional Information Argument		
Additional-information	C	12.2.1.3.1.6

12.2.1.3.1.1 Report-identifier

This argument contains an **MTS-identifier** that distinguishes the report from all other messages, probes and reports within the MTS. It shall be generated by the originating-MTA of the report.

12.2.1.3.1.2 Report-destination-name

This argument contains the **OR-name** of the immediate destination of the report. It shall be generated by the originating-MTA of the report, and subsequently modified by the DL expansion-points if any DLs had been expanded to add recipients to the subject.

The originating-MTA of the report shall set this argument to be the **originator-name** of the subject if the subject does not have a **DL-expansion-history**, or to the last **OR-name** in the **DL-expansion-history** if this is present in the subject.

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

A DL expansion-point may replace its own **OR-name** in this argument by the **OR-name** which immediately precedes its own **OR-name** in the report's **originator-and-DL-expansion-history**, or some other **OR-name** according to the reporting-policy of the DL.

12.2.1.3.1.3 Subject-identifier

This argument contains the **message-identifier** (or **probe-identifier**) of the subject (an **MTS-identifier**). It shall be generated by the originating-MTA of the subject.

12.2.1.3.1.4 Subject-intermediate-trace-information

This argument contains the **trace-information** present in the subject when it was transferred into the reporting-MD. It shall be present if, and only if, an audit-and-confirmed report was requested by the originating-MTA of the subject. It may be generated by the reporting-MTA.

Note – The inclusion in the **subject-intermediate-trace-information** of the **internal-trace-information** present in the subject when it was transferred to the reporting-MTA may be the subject of future standardisation.

12.2.1.3.1.5 Arrival-time

This argument contains the **Time** at which the subject entered the MD making the report. It shall be generated by the originating-MD of the report. A different value of this argument may be specified for each recipient of the subject to which the report relates.

12.2.1.3.1.6 Additional-information

The specification of the contents of this argument is by bilateral agreement between MDs.

12.2.1.3.2 Results

The Report-transfer abstract-operation does not return a result.

12.2.1.3.3 Abstract-errors

There are no abstract-errors that may disrupt the Report-transfer abstract-operation.

12.2.2 Abstract-errors

The transfer-port has no abstract-errors.

12.3 Common Parameter Types

This clause defines a number of common parameter types of the MTA Abstract Service.

12.3.1 Trace-information and internal-trace-information

Trace-information documents the actions taken on a message, probe or report by each MD through which it passes as it is transferred through the MTS.

Internal-trace-information documents the actions taken on a message, probe or report by each MTA through which it passes as it is transferred through an MD. **Internal-trace-information** may be removed from a message, probe or report before it is transferred out of an MD. An MD may (but is not required to) remove **internal-trace-information** relating to other MDs.

Trace-information (or **internal-trace-information**) comprises a sequence of **trace-information-elements** (or **internal-trace-information-elements**). The first **trace-information-element** (or **internal-trace-information-element**) is that supplied by the originating-MD (or -MTA) of the message, probe or report. The second **trace-information-element** (or **internal-trace-information-element**) is that supplied by the next MD (or MTA) encountered by the message, probe or report, and so on. Each MD (or MTA) adds its **trace-information-element** (or **internal-trace-information-element**) to the end of the existing sequence. **Trace-information** is added by the first MTA encountered by the message, probe or report in each MD that it passes through and, if necessary, modified by subsequent MTAs in that MD.

Each **trace-information-element** includes the **global-domain-identifier** of the MD supplying the **trace-information-element**.

Each **internal-trace-information-element** includes the **MTA-name** of the MTA supplying the **internal-trace-information-element** and the **global-domain-identifier** of the MD to which the MTA belongs.

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

Each **trace-information-element** (or **internal-trace-information-element**) includes the **arrival-time** at which the message, probe or report entered the MD (or MTA). In the case of the originating-MD (or -MTA) of the message, probe or report, the **arrival-time** is the time of message-submission, probe-submission or report generation, respectively.

Each **trace-information-element** (or **internal-trace-information-element**) specifies the **routing-action** the MD (or MTA) supplying the **trace-information-element** (or **internal-trace-information-element**) took with respect to the message, probe or report. **Relayed** is the normal **routing-action** of transferring the message, probe or report to another MD (or MTA). **Rerouted** indicates that an attempt had previously been made to route the message, probe or report to an **attempted-domain** (or **attempted-MTA**); the **global-domain-identifier** of the **attempted-domain** is included in the **trace-information-element**; if the rerouting attempt was to another MTA within the same MD, then the **MTA-name** of the **attempted-MTA** is included in the **internal-trace-information-element**; if the rerouting attempt was to another MD, then the **global-domain-identifier** of the **attempted-domain** is included in the **internal-trace-information-element** instead of an **MTA-name**.

Each **trace-information-element** (or **internal-trace-information-element**) also specifies any **additional-actions** the MD (or MTA) supplying the **trace-information-element** (or **internal-trace-information-element**) took with respect to the message, probe or report. Indications of any such **additional-actions** which appear in the **internal-trace-information-elements** during a traversal of an MD shall also be reflected in the corresponding **trace-information-element**(s) for the traversal of the MD.

If deferred-delivery caused the MD (or MTA) supplying the **trace-information-element** (or **internal-trace-information-element**) to hold the message for a period of time, the **deferred-time** when it started to process the message for delivery or transfer is also included in the **trace-information-element** (or **internal-trace-information-element**). This parameter is not present in **trace-information-elements** (or **internal-trace-information-elements**) on probes and reports.

If the MD (or MTA) supplying the **trace-information-element** (or **internal-trace-information-element**) subjects a message to conversion, the **converted-encoded-information-types** following the conversion is also included in the **trace-information-element** (or **internal-trace-information-element**). For a probe, an MD (or MTA) that would have converted the subject-message indicates the **encoded-information-types** the subject-message would contain after conversion in its **trace-information-element** (or **internal-trace-information-element**). This parameter is not present in **trace-information** (or **internal-trace-information**) on reports.

If the MD (or MTA) redirects a message, a probe or a report (for any, but not necessarily all, of a message's or probe's recipients), **redirected** is indicated in the **trace-information-element** (or **internal-trace-information-element**).

If the MD (or MTA) expands a DL of a message, **dl-operation** is indicated in the **trace-information-element** (or **internal-trace-information-element**). If the MD (or MTA) is a DL expansion-point and replaces its own **OR-name** in the **report-destination-name** of a report with another **OR-name** (see 12.2.1.3.1.2), **dl-operation** is indicated in the **trace-information-element** (or **internal-trace-information-element**) of the report. This parameter is not present in **trace-information** (or **internal-trace-information**) on probes.

Loop detection and suppression is done by an MD (or MTA) when it receives a message, probe or report from another MD (or MTA). Messages, probes and reports may legitimately re-enter an MD (or MTA) for several reasons (**rerouted**, etc) and consequently a message, probe or report may have several disjoint **trace-information-elements** (or **internal-trace-information-elements**) from the same MD (or MTA). Each time a message, probe or report is transferred through an MD (or MTA) the generation of **trace-information-elements** (or **internal-trace-information-elements**) is performed as follows:

i) one **trace-information-element** (or **internal-trace-information-element**) is added, marked as **relayed**;

ii) if a rerouting attempt is to occur, then the **trace-information-element** (or **internal-trace-information-element**) added in i) is modified to **rerouted** (and the number of **trace-information-elements** (or **internal-trace-information-elements**) added by the MD (or MTA) for this traversal of the MD (or MTA) remains at one);

iii) if subsequent attempts to reroute occur, then a new **trace-information-element** (or **internal-trace-information-element**) is added (marked as **rerouted**) to reflect each new rerouting attempt.

Several rerouting attempts to the same MD (or MTA) may occur.

Each **trace-information-element** (or **internal-trace-information-element**) added by an MD (or MTA) may contain indications of **additional-actions** performed by the MD (or MTA) on the message or probe (i.e., **deferred-time** (not present in **trace-information** (or **internal-trace-information**) on probes), **converted-encoded-information-types**, and either **redirected** or **dl-operation**). To indicate the order in which redirection and DL expansion have occurred, **redirected** and **dl-operation** indications shall not both appear in a single **trace-information-element** (or **internal-trace-information-element**).

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

13 Message Transfer Agent Abstract Syntax Definition

The abstract-syntax of the MTA Abstract Service is defined in Figure 4.

The abstract-syntax of the MTA Abstract Service is defined 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.

The abstract-syntax definition of the MTA Abstract Service has the following major parts:

Prologue: declarations of the exports from, and imports to, the MTA Abstract Service module (Figure 4 Part 1).

Objects and Ports: definitions of the MTA object and the transfer-port (Figure 4 Part 2).

MTA-bind and MTA-unbind: definitions of the MTA-bind and MTA-unbind used to establish and release associations between MTAs (Figure 4 Part 2).

Transfer Port: definitions of the transfer-port abstract-operations: Message-transfer, Probe-transfer and Report-transfer (Figure 4 Part 3).

Message Transfer Envelope: definition of the message-transfer-envelope (Figure 4 Part 3 to 4).

Probe Transfer Envelope: definition of the probe-transfer-envelope (Figure 4 Part 4).

Report Transfer Envelope & Content: definitions of the report-transfer-envelope and report-transfer-content (Figure 4 Part 5).

Envelope & Report Content Fields: definitions of envelope and report content fields (Figure 4 Parts 5 to 7).

Extension Fields: definitions of extension-fields (Figure 4 Part 7).

Common Parameters Types: definitions of common parameter types (Figure 4 Parts 7 to 8).

NOTE – The module implies a number of changes to the P1 protocol defined in CCITT Recommendation X.411 (1984). These changes are highlighted by means of underlining.

Each **extension-field** defined in Figure 4 (Part 6) carries with it an indication of its **criticality** for submission, transfer and delivery. The criticality mechanism is described in 9.2, and the procedures related to **extension-fields** and their **criticality** indications are further defined in clause 14.

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

```
MTAAbstractService { joint-iso-itu-t mhs(6) mts(3) modules(0) mta-abstract-service(2)
            version-1999(1) }

DEFINITIONS IMPLICIT TAGS ::=

BEGIN


--      Prologue

--      Exports everything

IMPORTS

        -- Remote Operations

        CONNECTION-PACKAGE, CONTRACT
                ----
                FROM Remote-Operations-Information-Objects {joint-iso-itu-t remote-operations(4)
                        informationObjects(5) version1(0) }

        emptyUnbind
                ----
                FROM Remote-Operations-Useful-Definitions {joint-iso-itu-t remote-operations(4)
                        useful-definitions(7) version1(0) }

        -- MTS Abstract Service Parameters

        ABSTRACT-ERROR, ABSTRACT-OPERATION, administration, AdministrationDomainName,
        certificate-selectors, certificate-selectors-override, Content, ContentIdentifier,
        ContentLength, ContentType, content-confidentiality-algorithm-identifier,
        content-correlator, content-integrity-check, conversion-with-loss-prohibited,
        ConvertedEncodedInformationTypes, CountryName, DeferredDeliveryTime, delivery,
        dl-exempted-recipients, dl-expansion-history, dl-expansion-prohibited,
        ExplicitConversion, EXTENSION, ExtensionField { }, GlobalDomainIdentifier,
        InitiatorCredentials, latest-delivery-time, message-origin-authentication-check,
        message-security-label, message-token, MHS-OBJECT, MTAName, MTSIdentifier,
        multiple-originator-certificates, ORAddressAndOptionalDirectoryName,
        OriginalEncodedInformationTypes, originator-and-DL-expansion-history,
        originator-certificate, originator-return-address, PerMessageIndicators,
        physical-delivery-modes, physical-delivery-report-request, physical-forwarding-address,
        physical-forwarding-address-request, physical-forwarding-prohibited,
        physical-rendition-attributes, PORT, Priority, PrivateDomainIdentifier,
        PrivateExtensions, probe-origin-authentication-check, proof-of-delivery,
        proof-of-delivery-request, recipient-certificate, recipient-number-for-advice,
        recipient-reassignment-prohibited, redirection-history, registered-mail-type,
        reporting-DL-name, reporting-MTA-certificate, reporting-MTA-name, ReportType,
        report-origin-authentication-check, requested-delivery-method, ResponderCredentials,
        SecurityContext, submission, SupplementaryInformation, Time
                ----
                FROM MTSAbstractService { joint-iso-itu-t mhs(6) mts(3) modules(0)
                        mts-abstract-service(1) version-1999(1) }

        -- IPM Information Objects

        IPMPerRecipientEnvelopeExtensions
                ----
                FROM IPMSInformationObjects { joint-iso-itu-t mhs(6) ipms(1) modules(0)
                        information-objects(2) version-1999(1) }

        -- Object Identifiers

        id-cp-mta-connect, id-ct-mta-transfer, id-ot-mta, id-pt-transfer
                ----
                FROM MTSObjectIdentifiers { joint-iso-itu-t mhs(6) mts(3) modules(0)
                        object-identifiers(0) version-1999(1) }
```

Figure 4 – Abstract Syntax Definition of the MTA Abstract Service (Part 1 of 8)

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

```
        -- Upper Bounds

        ub-bit-options, ub-integer-options, ub-recipients, ub-transfers
                ----
                FROM MTSUpperBounds { joint-iso-itu-t mhs(6) mts(3) modules(0) upper-bounds(3)
                        version-1999(1) };

--      Objects

mta MHS-OBJECT ::= {
        BOTH  { mta-transfer }
        ID    id-ot-mta }

--      Contracts

mta-transfer CONTRACT ::= {
        CONNECTION     mta-connect
        OPERATIONS OF  { transfer }
        ID             id-ct-mta-transfer }

--      Connection package

mta-connect CONNECTION-PACKAGE ::= {
        BIND        mta-bind
        UNBIND      mta-unbind
        ID          id-cp-mta-connect }

--      Ports

transfer PORT ::= {
        OPERATIONS  { message-transfer | probe-transfer | report-transfer }
        ID          id-pt-transfer }

--      MTA-bind and MTA-unbind

mta-bind ABSTRACT-OPERATION ::= {
        ARGUMENT  MTABindArgument
        RESULT    MTABindResult
        ERRORS    { mta-bind-error } }

mta-unbind ABSTRACT-OPERATION ::= emptyUnbind

MTABindArgument ::= CHOICE {
        unauthenticated NULL,        -- if no authentication is required
        authenticated [1] SET {      -- if authentication is required
                initiator-name [0] MTAName,
                initiator-credentials [1] InitiatorCredentials (WITH COMPONENTS { ... ,
                                protected ABSENT } ),
                security-context [2] SecurityContext OPTIONAL } }

MTABindResult ::= CHOICE {
        unauthenticated NULL,        -- if no authentication is required
        authenticated [1] SET {      -- if authentication is required
                responder-name [0] MTAName,
                responder-credentials [1] ResponderCredentials (WITH COMPONENTS { ... ,
                                protected ABSENT } ) } }

mta-bind-error ABSTRACT-ERROR ::= {
        PARAMETER  INTEGER {
                busy (0),
                authentication-error (2),
                unacceptable-dialogue-mode (3),
                unacceptable-security-context (4),
                inadequate-association-confidentiality (5) } (0..ub-integer-options) }
```

Figure 4 – Abstract Syntax Definition of the MTA Abstract Service (Part 2 of 8)

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

```
--      Transfer Port

message-transfer ABSTRACT-OPERATION ::= {
       ARGUMENT Message }

probe-transfer ABSTRACT-OPERATION ::= {
       ARGUMENT Probe }

report-transfer ABSTRACT-OPERATION ::= {
       ARGUMENT Report }

Message ::= SEQUENCE {
              envelope MessageTransferEnvelope,
              content Content }

Probe ::= ProbeTransferEnvelope

Report ::= SEQUENCE {
              envelope ReportTransferEnvelope,
              content ReportTransferContent }

--      Message Transfer Envelope

MessageTransferEnvelope ::= SET {
       COMPONENTS OF PerMessageTransferFields,
       per-recipient-fields [2] SEQUENCE SIZE (1..ub-recipients) OF
              PerRecipientMessageTransferFields }

PerMessageTransferFields ::= SET {
       message-identifier MessageIdentifier,
       originator-name OriginatorName,
       original-encoded-information-types OriginalEncodedInformationTypes OPTIONAL,
       content-type ContentType,
       content-identifier ContentIdentifier OPTIONAL,
       priority Priority DEFAULT normal,
       per-message-indicators PerMessageIndicators DEFAULT { },
       deferred-delivery-time [0] DeferredDeliveryTime OPTIONAL,
       per-domain-bilateral-information [1] SEQUENCE SIZE (1..ub-transfers) OF
              PerDomainBilateralInformation OPTIONAL,
       trace-information TraceInformation,
       extensions [3] SET OF ExtensionField {{ MessageTransferExtensions }} DEFAULT { } }

MessageTransferExtensions EXTENSION ::= {
       -- May contain the following extensions, private extensions, and future standardised extensions,
       -- at most one instance of each extension type:
       recipient-reassignment-prohibited |
       dl-expansion-prohibited |
       conversion-with-loss-prohibited |
       latest-delivery-time |
       originator-return-address |
       originator-certificate |
       content-confidentiality-algorithm-identifier |
       message-origin-authentication-check |
       message-security-label |
       content-correlator |
       dl-exempted-recipients |
       certificate-selectors |
       multiple-originator-certificates |
       dl-expansion-history |
       internal-trace-information |
       PrivateExtensions, ... }

PerRecipientMessageTransferFields ::= SET {
       recipient-name RecipientName,
       originally-specified-recipient-number [0] OriginallySpecifiedRecipientNumber,
       per-recipient-indicators [1] PerRecipientIndicators,
       explicit-conversion [2] ExplicitConversion OPTIONAL,
       extensions [3] SET OF ExtensionField {{ PerRecipientMessageTransferExtensions }}
                                                                    DEFAULT { } }
```

Figure 4 – Abstract Syntax Definition of the MTA Abstract Service (Part 3 of 8)

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

```
PerRecipientMessageTransferExtensions EXTENSION ::= {
        -- May contain the following extensions, private extensions, and future standardised extensions,
        -- at most one instance of each extension type:
        originator-requested-alternate-recipient |
        requested-delivery-method |
        physical-forwarding-prohibited |
        physical-forwarding-address-request |
        physical-delivery-modes |
        registered-mail-type |
        recipient-number-for-advice |
        physical-rendition-attributes |
        physical-delivery-report-request |
        message-token |
        content-integrity-check |
        proof-of-delivery-request |
        certificate-selectors-override |
        recipient-certificate |
        redirection-history |
        IPMPerRecipientEnvelopeExtensions |
        PrivateExtensions, ... }

--      Probe Transfer Envelope

ProbeTransferEnvelope ::= SET {
        COMPONENTS OF PerProbeTransferFields,
        per-recipient-fields [2] SEQUENCE SIZE (1..ub-recipients) OF
PerRecipientProbeTransferFields}

PerProbeTransferFields ::= SET {
        probe-identifier ProbeIdentifier,
        originator-name OriginatorName,
        original-encoded-information-types OriginalEncodedInformationTypes OPTIONAL,
        content-type ContentType,
        content-identifier ContentIdentifier OPTIONAL,
        content-length [0] ContentLength OPTIONAL,
        per-message-indicators PerMessageIndicators DEFAULT { },
        per-domain-bilateral-information [1] SEQUENCE SIZE (1..ub-transfers) OF
                PerDomainBilateralInformation OPTIONAL,
        trace-information TraceInformation,
        extensions [3] SET OF ExtensionField {{ ProbeTransferExtensions }} DEFAULT { } }

ProbeTransferExtensions EXTENSION ::= {
        -- May contain the following extensions, private extensions, and future standardised extensions,
        -- at most one instance of each extension type:
        recipient-reassignment-prohibited |
        dl-expansion-prohibited |
        conversion-with-loss-prohibited |
        originator-certificate |
        message-security-label |
        content-correlator |
        probe-origin-authentication-check |
        internal-trace-information |
        PrivateExtensions, ... }

PerRecipientProbeTransferFields ::= SET {
        recipient-name RecipientName,
        originally-specified-recipient-number [0] OriginallySpecifiedRecipientNumber,
        per-recipient-indicators [1] PerRecipientIndicators,
        explicit-conversion [2] ExplicitConversion OPTIONAL,
        extensions [3] SET OF ExtensionField {{ PerRecipientProbeTransferExtensions }}
                                                                        DEFAULT { } }

PerRecipientProbeTransferExtensions EXTENSION ::= {
        -- May contain the following extensions, private extensions, and future standardised extensions,
        -- at most one instance of each extension type:
        originator-requested-alternate-recipient |
        requested-delivery-method |
        physical-rendition-attributes |
        redirection-history |
        PrivateExtensions, ... }
```

Figure 4 – Abstract Syntax Definition of the MTA Abstract Service (Part 4 of 8)

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

```
--      Report Transfer Envelope

ReportTransferEnvelope ::= SET {
        report-identifier ReportIdentifier,
        report-destination-name ReportDestinationName,
        trace-information TraceInformation,
        extensions [1] SET OF ExtensionField {{ ReportTransferEnvelopeExtensions }}
                                                                        DEFAULT { } }

ReportTransferEnvelopeExtensions EXTENSION ::= {
        -- May contain the following extensions, private extensions, and future standardised extensions,
        -- at most one instance of each extension type:
        message-security-label |
        redirection-history |
        originator-and-DL-expansion-history |
        reporting-DL-name |
        reporting-MTA-certificate |
        report-origin-authentication-check |
        internal-trace-information |
        reporting-MTA-name |
        PrivateExtensions, ... }

--      Report Transfer Content

ReportTransferContent ::= SET {
        COMPONENTS OF PerReportTransferFields,
        per-recipient-fields [0] SEQUENCE SIZE (1..ub-recipients) OF
                PerRecipientReportTransferFields}

PerReportTransferFields ::= SET {
        subject-identifier SubjectIdentifier,
        subject-intermediate-trace-information SubjectIntermediateTraceInformation OPTIONAL,
        original-encoded-information-types OriginalEncodedInformationTypes OPTIONAL,
        content-type ContentType OPTIONAL,
        content-identifier ContentIdentifier OPTIONAL,
        returned-content [1] Content OPTIONAL,
        additional-information [2] AdditionalInformation OPTIONAL,
        extensions [3] SET OF ExtensionField {{ ReportTransferContentExtensions }}
                                                                        DEFAULT { } }

ReportTransferContentExtensions EXTENSION ::= {
        -- May contain the following extensions, private extensions, and future standardised extensions,
        -- at most one instance of each extension type:
        content-correlator |
        PrivateExtensions, ... }

PerRecipientReportTransferFields ::= SET {
        actual-recipient-name [0] ActualRecipientName,
        originally-specified-recipient-number [1] OriginallySpecifiedRecipientNumber,
        per-recipient-indicators [2] PerRecipientIndicators,
        last-trace-information [3] LastTraceInformation,
        originally-intended-recipient-name [4] OriginallyIntendedRecipientName OPTIONAL,
        supplementary-information [5] SupplementaryInformation OPTIONAL,
        extensions [6] SET OF ExtensionField {{ PerRecipientReportTransferExtensions }}
                                                                        DEFAULT { } }

PerRecipientReportTransferExtensions EXTENSION ::= {
        -- May contain the following extensions, private extensions, and future standardised extensions,
        -- at most one instance of each extension type:
        redirection-history |
        physical-forwarding-address |
        recipient-certificate |
        proof-of-delivery |
        PrivateExtensions, ... }

--      Envelope & Report Content Fields

MessageIdentifier ::= MTSIdentifier

OriginatorName ::= ORAddressAndOptionalDirectoryName
```

Figure 4 – Abstract Syntax Definition of the MTA Abstract Service (Part 5 of 8)

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

```
PerDomainBilateralInformation ::= SEQUENCE {
       COMPONENTS OF BILATERAL.&id,
       bilateral-information BILATERAL.&Type }

BILATERAL ::= CLASS {
       &id BilateralDomain UNIQUE,
       &Type }
WITH SYNTAX { &Type, IDENTIFIED BY &id }

BilateralDomain ::= SEQUENCE {
       country-name CountryName,
       domain CHOICE {
              administration-domain-name AdministrationDomainName,
              private-domain SEQUENCE {
                     administration-domain-name [0] AdministrationDomainName,
                     private-domain-identifier [1] PrivateDomainIdentifier } } }

RecipientName ::= ORAddressAndOptionalDirectoryName

OriginallySpecifiedRecipientNumber ::= INTEGER (1..ub-recipients)

PerRecipientIndicators ::= BIT STRING {
       responsibility (0),
       -- responsible 'one', not-responsible 'zero'
       originating-MTA-report (1),
       originating-MTA-non-delivery-report (2),
       -- either originating-MTA-report, or originating-MTA-non-delivery-report,
       -- or both, shall be 'one':
       -- originating-MTA-report bit 'one' requests a 'report';
       -- originating-MTA-non-delivery-report bit 'one' requests a 'non-delivery-report';
       -- both bits 'one' requests an 'audited-report';
       -- bits 0 - 2 'don't care' for Report Transfer Content
       originator-report (3),
       originator-non-delivery-report (4),
       -- at most one bit shall be 'one':
       -- originator-report bit 'one' requests a 'report';
       -- originator-non-delivery-report bit 'one' requests a 'non-delivery-report';
       -- both bits 'zero' requests 'no-report'
       reserved-5 (5),
       reserved-6 (6),
       reserved-7 (7)
       -- reserved- bits 5 - 7 shall be 'zero' -- } (SIZE (8..ub-bit-options))

ProbeIdentifier ::= MTSIdentifier

ReportIdentifier ::= MTSIdentifier

ReportDestinationName ::= ORAddressAndOptionalDirectoryName

SubjectIdentifier ::= MessageOrProbeIdentifier

MessageOrProbeIdentifier ::= MTSIdentifier

SubjectIntermediateTraceInformation ::= TraceInformation

--      AdditionalInformation is retained for backwards compatibility only,
--      and use in new systems is strongly deprecated

ADDITIONAL ::= CLASS { &Type }

AdditionalInformation ::= ADDITIONAL.&Type  -- maximum ub-additional-info octets including all encoding

ActualRecipientName ::= ORAddressAndOptionalDirectoryName
```

Figure 4 – Abstract Syntax Definition of the MTA Abstract Service (Part 6 of 8)

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

```
LastTraceInformation ::= SET {
       arrival-time [0] ArrivalTime,
       converted-encoded-information-types ConvertedEncodedInformationTypes OPTIONAL,
       report-type [1] ReportType }

OriginallyIntendedRecipientName ::= ORAddressAndOptionalDirectoryName


--      Extension Fields

originator-requested-alternate-recipient EXTENSION ::= {
       OriginatorRequestedAlternateRecipient,
       IDENTIFIED BY standard-extension:2 }

OriginatorRequestedAlternateRecipient ::= ORAddressAndOptionalDirectoryName

trace-information EXTENSION ::= {
       TraceInformation,
       IDENTIFIED BY standard-extension:37 }

internal-trace-information EXTENSION ::= {
       InternalTraceInformation,
       IDENTIFIED BY standard-extension:38 }

InternalTraceInformation ::= SEQUENCE SIZE (1..ub-transfers) OF
InternalTraceInformationElement

InternalTraceInformationElement ::= SEQUENCE {
       global-domain-identifier GlobalDomainIdentifier,
       mta-name MTAName,
       mta-supplied-information MTASuppliedInformation }

MTASuppliedInformation ::= SET {
       arrival-time [0] ArrivalTime,
       routing-action [2] RoutingAction,
       attempted CHOICE {
              mta MTAName,
              domain GlobalDomainIdentifier } OPTIONAL,
       -- additional-actions -- COMPONENTS OF InternalAdditionalActions }

InternalAdditionalActions ::= AdditionalActions


--      Common Parameter Types

TraceInformation ::= [APPLICATION 9] SEQUENCE SIZE (1..ub-transfers) OF
TraceInformationElement

TraceInformationElement ::= SEQUENCE {
       global-domain-identifier GlobalDomainIdentifier,
       domain-supplied-information DomainSuppliedInformation }

DomainSuppliedInformation ::= SET {
       arrival-time [0] ArrivalTime,
       routing-action [2] RoutingAction,
       attempted-domain GlobalDomainIdentifier OPTIONAL,
       -- additional-actions -- COMPONENTS OF AdditionalActions }

AdditionalActions ::= SET {
       deferred-time [1] DeferredTime OPTIONAL,
       converted-encoded-information-types ConvertedEncodedInformationTypes OPTIONAL,
       other-actions [3] OtherActions DEFAULT { } }

RoutingAction ::= ENUMERATED {
       relayed (0),
       rerouted (1) }
```

Figure 4 – Abstract Syntax Definition of the MTA Abstract Service (Part 7 of 8)

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

```
DeferredTime ::= Time

ArrivalTime ::= Time

OtherActions ::= BIT STRING {
       redirected (0),
       dl-operation (1) } (SIZE (0..ub-bit-options))

END     -- of MTA Abstract Service
```

Figure 4 – Abstract Syntax Definition of the MTA Abstract Service (Part 8 of 8)

SECTION FOUR – PROCEDURES FOR DISTRIBUTED OPERATION OF THE MTS

14 Procedures for Distributed Operation of the MTS

This clause specifies the procedures for distributed operation of the MTS, which are performed by MTAs. Each MTA individually performs the procedures described below; the collective action of all MTAs provides the MTS Abstract Service to the users of the MTS.

Although the procedures include most of the important actions required of an MTA, considerable detail has been omitted for clarity of exposition and to avoid unnecessary redundancy. The abstract-service definitions should be consulted for a definitive treatment of MTA actions.

14.1 Overview of the MTA Model

14.1.1 Organization and Modelling Technique

The description of procedures for a single MTA is based on the model shown in Figures 5 through 11 and described below. It should be noted that the model is included for descriptive purposes only and is not intended to constrain in any way the implementation of an MTA.

Neither the procedures shown nor the order of processing steps in them necessarily imply specific characteristics of an actual MTA.

The model distinguishes between *modules* and *procedures*. *Modules*, in the sense used here, are autonomous processing entities which can be invoked by other modules or by events external to the MTA, and which can in turn invoke other modules or generate external events. Modules are not bound together by an explicitly described control structure; rather the control structure among modules arises from their pattern of cross invocations. Modules correspond to *objects* in the sense of object-oriented programming.

Procedures are used here in the conventional programming sense. Procedures are task or function oriented. Procedures can call other procedures, subroutine fashion, with control returning to the calling procedure when the called procedure has completed. Such calls can be nested to arbitrary depth, and a procedure can call itself recursively. Procedures are bound together by explicitly defined control structures built from procedure calls and such conventional programming devices as iteration and conditional execution.

In the model procedures exist within modules. Each module contains at least one procedure and can contain several. In the latter case, the procedures and governing control structure are described explicitly. In the former case the existence of a module's single procedure is usually treated as implicit.

Using these modelling techniques, an MTA application process can be refined as follows: for each abstract-operation (whether consumer or supplier) that can exist between an MTA and the MTS-users it serves, or between an MTA and the other MTAs with which it cooperates there is a single module called an *external module*. The set of external modules is responsible for the input and output of messages, probes, and reports into and out of the MTA and for the support of such operations as MTS-bind, MTS-unbind, Register, Submission-control and Delivery-control. The external modules are shown in Figure 5 and described in clauses 14.5 through 14.10, grouped by port.

In order to perform the various abstract-operations for which it is responsible, an MTA must perform certain processing operations on each message, probe, or report that enters, or originates within it. In the model these are the province of *internal modules*, shown in Figure 6 and described in clauses 14.2 through 14.4.

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

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

The external and internal modules relate to one another as follows: an external module communicates only with an internal module, and not with another external module or directly with a procedure within an internal module. Thus, the internal modules not only support the bulk of processing within an MTA, but also serve as links between its external modules. In addition to the internal modules Figure 6 also shows the external modules with which they communicate.

The MTA is event driven in that it remains quiescent until an event is detected on one of its ports. Many events, such as the invocation of a MTS-bind, Submission-control, Delivery-control or Register abstract-operation by an MTS-user or another MTA, are dealt with directly and completely by the module assigned to that abstract-operation. However other events trigger processing that can reverberate through the MTA, endure over time and ultimately trigger one or more output events. It is these events that engage the internal processing modules. They are:

a) A message or probe originated by a locally supported MTS-user enters via the submission-port.

b) A message, probe or report relayed from another MTA enters via the transfer-port.

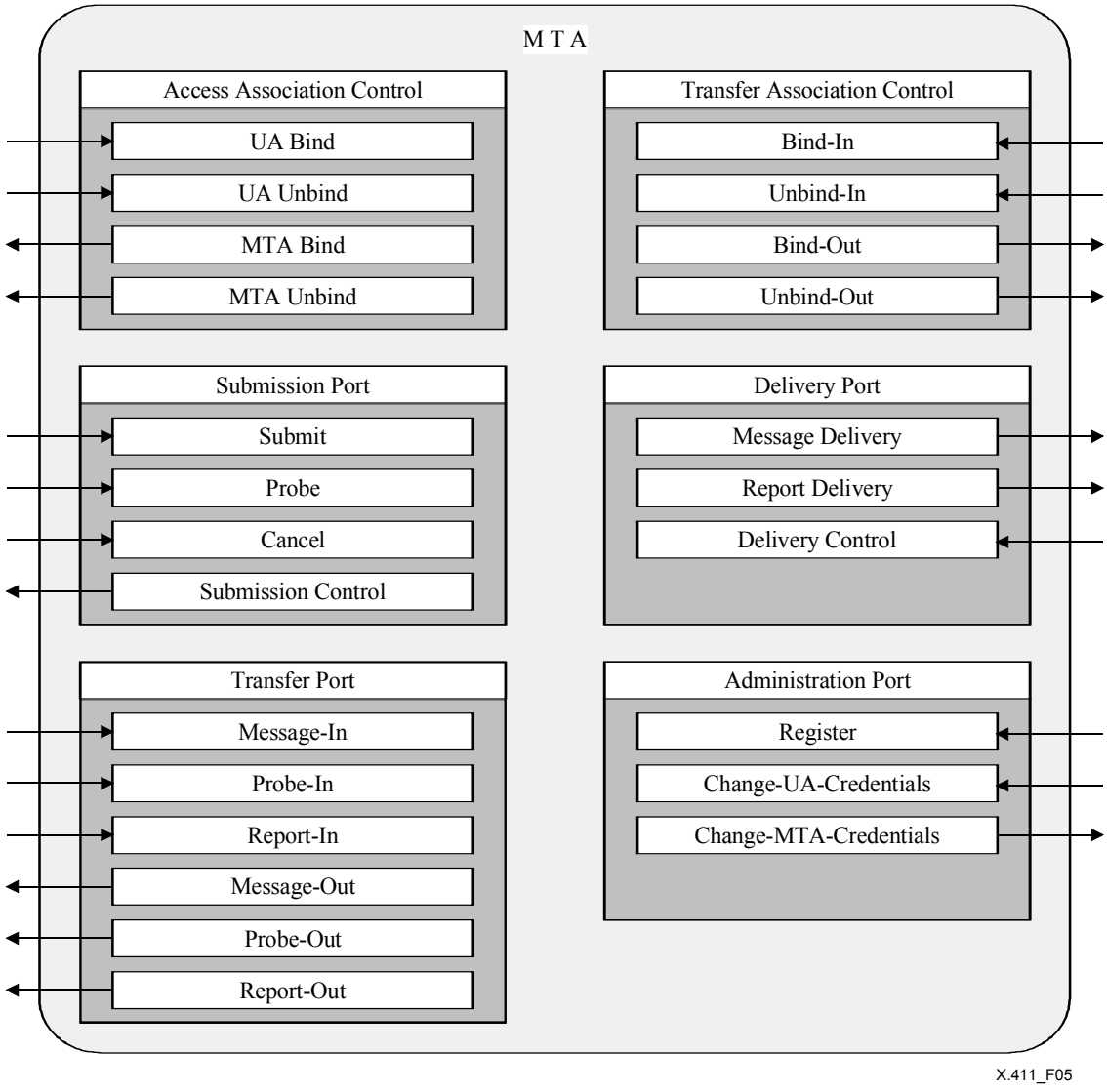


Figure 5 – Ports and modules of an MTA

Because the processing within an MTA can become rather complex, especially for messages with multiple recipients, the model assumes, as an internal bookkeeping device, that each message carries with it a set of instructions, one for the message as a whole, and one for each recipient. These instructions help guide a message through the processing steps and convey information between the modules and procedures internal to the MTA.

NOTE 1 – The procedures described herein focus on the processing of a single message. This is adequate in all but one respect: the queuing of messages and the relative priority of procedure invocation are driven explicitly by the argument **priority** in case of a message which enters via the submission- or the transfer-port, or implicitly (of urgent priority) in the case of a report or a probe which is generated internally or enters via the transfer-port.

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

NOTE 2 – An MTA can specify several default delivery time windows for each message priority [e.g. those values defined in the F.400 series Recommendations[]. The MTS and therefore each MTA involved should take such values into account during message processing. For example, the MTA can apply a maximum delivery deadline. If that time period expires prior to delivery, the MTA generates a non-delivery-report and discards the message. The required actions in this case are identical to the actions required when **latest-delivery-time** is reached.

NOTE 3 – The discussion of trace-information is incomplete due to its complex nature. Some important details are highlighted but the complete and definitive treatment of trace-information appears in 12.3.1.

NOTE 4 – ITU-T Rec. X.412 ISO/IEC 10021-10 specifies some additions to and replacements of some of the procedures in this Service Definition, which are applicable to MTAs which claim conformance to ITU-T Rec. X.412 ISO/IEC 10021-10.

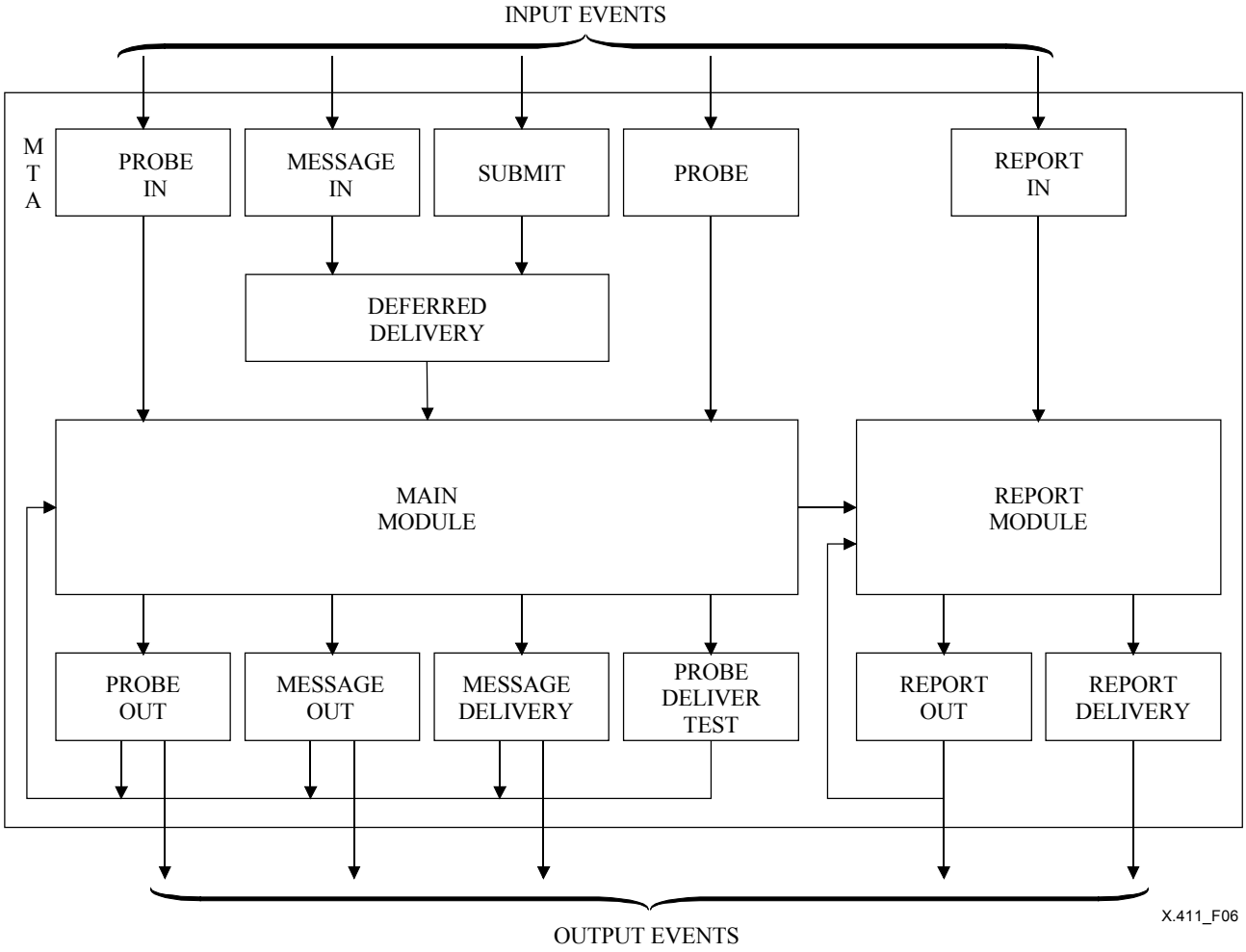


Figure 6 – Relationship of internal and external modules

14.2 Deferred Delivery Module

This module provides the Deferred Delivery element-of-service. It is invoked by the Message-submission and Message-in modules which pass a message to be checked for deferred delivery request and held if necessary. It invokes the Main module, passing on the message upon completion of its single internal procedure.

14.2.1 Deferred Delivery Procedure

14.2.1.1 Arguments

A message to be checked for deferred delivery request and held if necessary.

14.2.1.2 Results

The message is returned. If deferral occurred, an arrival timestamp accompanies the message.

14.2.1.3 Errors

The message with instructions detailing the problem encountered.

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

14.2.1.4 Procedure Description

1) The message is checked for presence of the **deferred-delivery-time** field. If absent the procedure returns the message and terminates. If present the **deferred-delivery-time** is checked against the current time. If the **deferred-delivery-time** has expired, the procedure returns the message with the **deferred-delivery-time** field removed and terminates.

2) This step applies only to a message from the Message-in module. The MTA checks for a bilateral agreement requiring it to provide deferred delivery for this message. If there is such an agreement, processing continues at step 3. If there is no such agreement, then one of the following is performed:

   a) The procedure returns the message without deferring it, and then terminates;

   b) The procedure returns the message with an instruction with a **non-delivery-reason-code** of **deferred-delivery-not-performed** and a **non-delivery-diagnostic-code** of **no-bilateral-agreement**. The procedure then terminates.

3) Depending upon policy, one of the following is performed:

   a) If there is a bilateral agreement with the domain(s) or MTA(s) to which the message will be transferred, that those domain(s) or MTA(s) will take responsibility for the deferral request, then the procedure returns the message without deferring it. The procedure then terminates;

   b) The current time is noted as the message arrival time, and the message is held until expiration of the **deferred-delivery-time**. The message with the **deferred-delivery-time** field removed and the arrival timestamp are then returned, and the procedure terminates.

NOTE – It is necessary to remove the **deferred-delivery-time** field once deferral is completed so that when the message is transferred to another domain or MTA there is no danger of non-delivery (see step 2 b) if the clocks are out of synchronization.

14.3 Main Module

The Main module performs the bulk of processing on messages and probes entering the MTA. Figure 6 shows the relationships between the Main module and the modules which it can invoke or be invoked by. The Main module is subject to invocation by:

1) the Probe-in module, which passes a probe;
2) the Deferred-delivery module, which passes a message;
3) the Probe module, which passes a probe.

In the case of an error condition or the need for a positive delivery report, the Main module can also be invoked by:

4) the Message-out module, which passes a message with per-message instruction indicating the problem encountered;
5) the Probe-out module, which passes a probe with per-message instruction indicating the problem encountered;
6) the Message-delivery module, which passes a message with per-recipient instructions indicating the problem(s) and/or success(es) encountered;
7) The Probe-delivery-test module, which passes a probe with per-recipient instructions indicating the problem(s) or success(es) encountered.
8) The Deferred-delivery module, which passes a message with instructions indicating the problem encountered.

The Main module contains procedures which, collectively, support the following functions:

Trace processing
Loop detection
Routing and re-routing
Recipient redirection
Content conversion
Distribution list expansion
Message replication
Origin authentication of messages and probes
Name resolution.

The procedures that perform these functions are called by a single Control procedure that guides the processing of each message or probe received by the Main module. Figure 7 shows the organization of the Control and subsidiary procedures within the Main module; Figure 8 shows the flow of information through these procedures.

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

For each message or probe received, the Main module calls the Control procedure with that message or probe as argument. As result, the Control procedure returns one or more replicas of the message or probe with appropriate instructions attached. Depending on the nature of these instructions the Main module then invokes:

1) the Message-out module, to which it passes each message with a per-message transfer instruction;
2) the Probe-out module, to which it passes each probe with a per-message transfer instruction;
3) the Message-delivery module, to which it passes each message with one or more per-recipient delivery instructions;
4) the Probe-delivery-test module, to which it passes each probe with one or more per-recipient delivery instructions;
5) the Report module, to which it passes each message or probe with a per-message instruction and/or one or more per-recipient instructions indicating report generation.

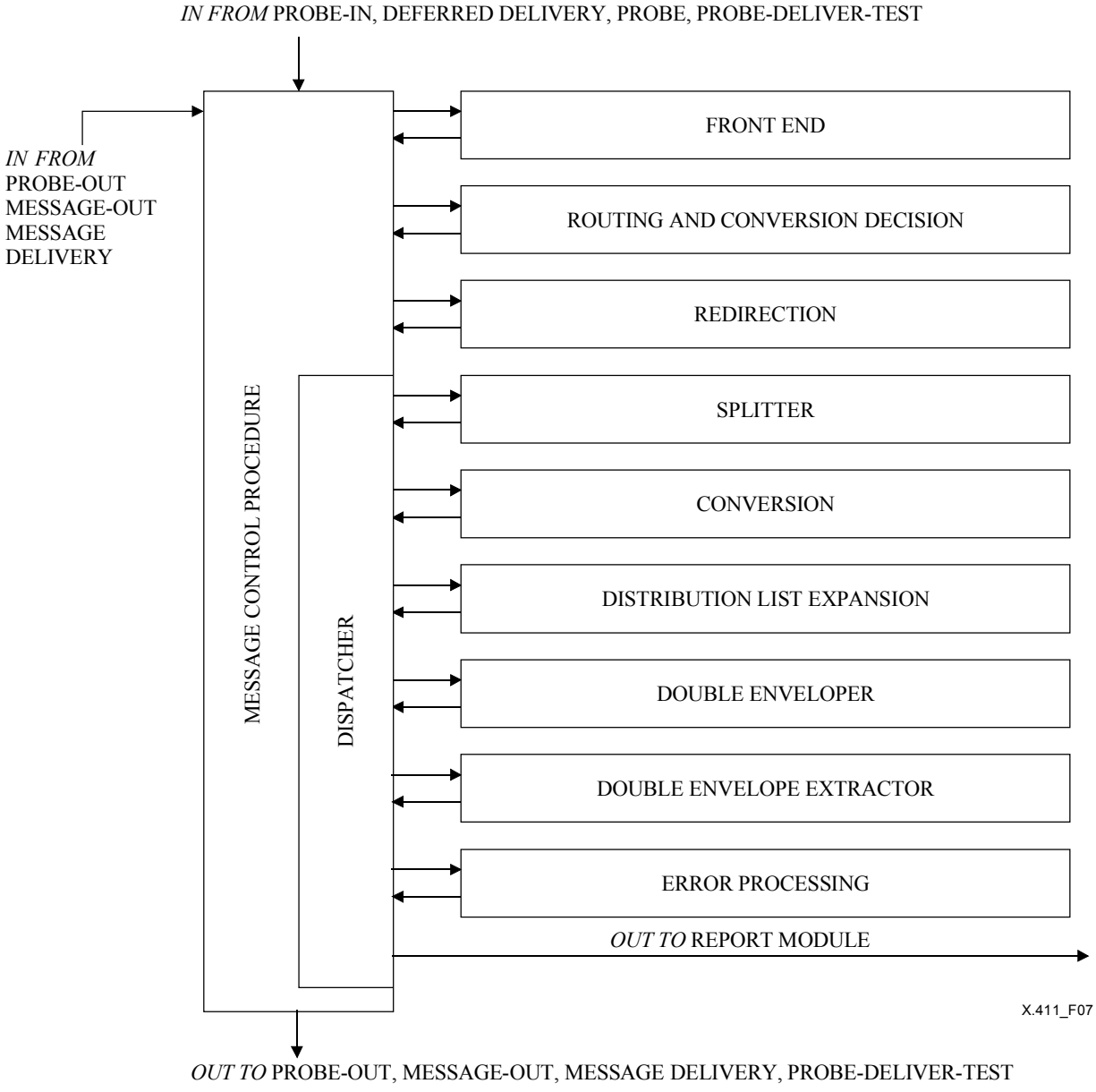
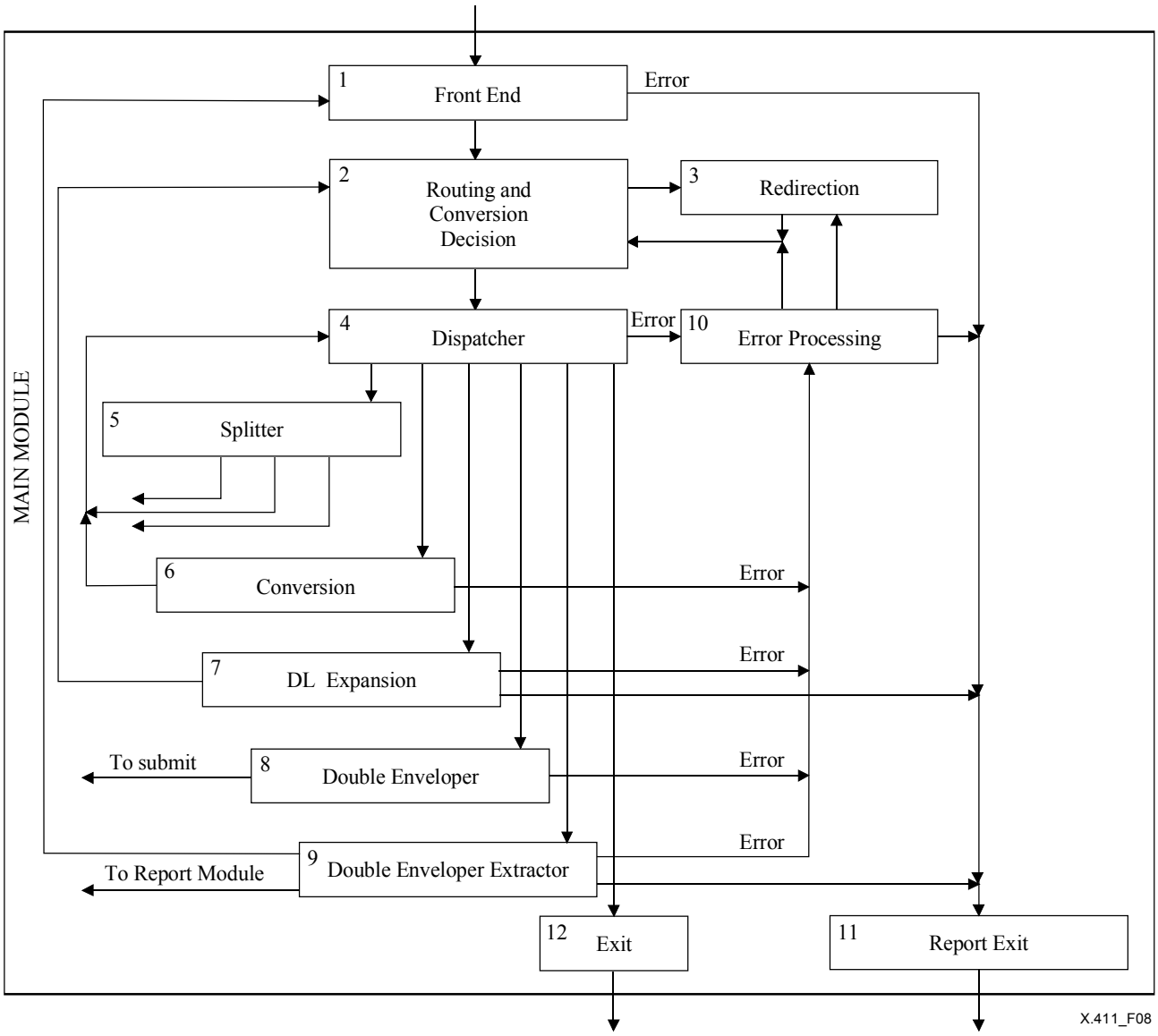


Figure 7 – Organisation of Procedures within the Main Module

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



NOTE – Numbers in this figure refer to the numbered steps in the control procedures logic (see 14.3.1.4).

Figure 8 – Information Flow within the Main Module

14.3.1 Control Procedure

This procedure directs each incoming message or probe through the remaining procedures of the Main module. The overall flow of information is shown in Figure 8.

14.3.1.1 Arguments

One of the following (these arguments correspond to the messages and probes that can be passed to the Main module upon invocation):

1) A message or probe without instructions (from the Probe-in or Probe module);
2) A message without instructions but with optional arrival timestamp (from the Deferred-delivery module);
3) A message or probe with per-message instruction describing a transfer problem (from the Message-out or Probe-out module);
4) A message or probe with per-recipient instructions describing delivery problems or successes (from the Message-delivery or Probe-delivery-test module).

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

14.3.1.2 Results

1) One or more replicas of the message or probe argument each accompanied by a per-message instruction indicating transfer;

and/or

2) one or more replicas of the message or probe argument each accompanied by one or more per-recipient instructions indicating delivery or delivery test;

and/or

3) one or more replicas of the message or probe argument each accompanied by one or more per-recipient instructions indicating report generation.

14.3.1.3 Errors

None. Error conditions are accounted for in the results described above.

14.3.1.4 Procedure Description

1) A message or probe without instructions:

   The Front-end procedure is first called to perform trace initialisation and several per-message checks such as message expiration and routing loop detection.

   Upon a return with report instruction indicating a problem with the message, processing continues at step 11.

   On all other returns processing continues below.

2) Routing-and-conversion-decision procedure is called to compute per-recipient routing and conversion instructions. (These are complete instructions that will direct the message or probe through the remainder of the procedures.)

   If a redirection instruction is indicated (e.g., **recipient-assigned-alternate-recipient**), processing continues at step 3.

   Otherwise, processing continues at step 4 (Dispatcher).

3) Redirection is called. Upon successful return, processing continues at step 2.

   In the case of an unsuccessful return, processing continues at step 10 (Error-handler).

4) Dispatcher. The Dispatcher acts on the generated instructions and passes control to the first of the following procedures that is applicable:

   – Splitting (step 5);
   – Conversion (step 6);
   – Distribution-list-expansion (step 7);
   – Double-enveloping (step 8);
   – Double-envelope-extraction (step 9);
   – Error-processing (step 10) in case the decision process encountered a problem, e.g., routing error;
   – Exit (step 12).

5) Splitter is called for replication as required by the per-recipient instructions generated in Routing-and-conversion-decision procedure. For each replica processing continues individually at step 4 (dispatcher).

6) Conversion is called for each message or probe needing conversion.

   Upon successful return of the message or probe, processing continues at step 4 (Dispatcher).

   Upon return with report instruction indicating a conversion error, processing continues at step 10 (Error-handler).

7) The DL-expansion procedure is called.

   Upon successful return of a message, processing continues at step 2 so that the recipients resulting from DL expansion can be properly dealt with.

   If a copy of the message with delivery report instructions is returned, in place of or in addition to the above return, its processing continues at step 11.

   A probe returning successfully will have report instructions; processing continues at step 11 (Report-generation).

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

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

Upon return of a message or probe with report instruction indicating DL expansion Error-processing continues at step 10.

8) The Double-enveloper procedure is called if the routing instruction requires the message to be embedded within an **inner-envelope content-type**.

   In the case of a successful return the procedure terminates, as the MTA has no further processing to perform on the original message.

   In the case of an unsuccessful return, processing continues at step 10 (Error-handler).

9) The Double-envelope-extractor procedure is called if the routing instruction is to extract the inner envelope from the **content**.

   Upon successful return of an extracted message or probe, processing of the extracted message or probe resumes at step 1. Upon successful return of an extracted report, processing of the extracted report continues as specified in 14.4.1. In addition in each case, processing of the report instructions on the original message continues at step 11.

   Upon an unsuccessful return, processing continues at step 10 (Error-handler).

10) This is the collection point that processing reaches upon detection that a message or probe cannot be handled by the main line procedures. The Error-processing procedure is called to seek another delivery method or a replacement recipient. Upon successful return the Error-processing procedure indicates the new recipient in an instruction to the Routing-and-conversion-decision procedure (step 2), where processing continues.

    If redirection is not possible, the message or probe is passed to the report generator (step 11).

11) The Control procedure terminates at this point and returns a message or probe with report generation instructions.

12) When a message or probe reaches this point the Control procedure terminates.

14.3.2 Front-end Procedure

This procedure performs trace initialisation, detection of message expiration, initial security check, loop detection, and criticality check.

14.3.2.1 Arguments

A message or probe and an optional arrival timestamp.

14.3.2.2 Results

The message, or probe with initialised trace information for this MTA.

14.3.2.3 Errors

The message or probe with report generation instructions detailing the problem encountered.

14.3.2.4 Procedure Description

1) If the message has crossed a domain boundary, a **trace-information-element** for this domain is added with **relay** as action. If an arrival time accompanies the message, then delivery deferral has occurred and **deferred-time** is set to the current time and **arrival-time** is set to the accompanying timestamp value. Otherwise no deferral has occurred and the **arrival-time** is set to the current time. An **internal-trace-information-element** is also added whether or not the message has crossed a domain boundary.

2) If required by the security policy in force and/or if the **message-origin-authentication-check** is incorrect, the procedure returns a report generation instruction. The values of the **non-delivery-reason-code** and **non-delivery-diagnostic-code** are set to **unable-to-transfer**, and **secure-messaging-error**, respectively.

3) If any of the **per-message** extension fields, or the **per-recipient** extension fields for recipients for which **responsibility** is set to **responsible**, is marked **critical-for-transfer** but is not semantically understood by the MTA, the procedure returns a report generation instruction for those recipients. If report generation instructions have been generated for some (but not all) recipients for which **responsibility** has the value **responsible**, then an instruction to split the message is returned. The **non-delivery-reason-code** is set to **unable-to-transfer** and the **non-delivery-diagnostic-code** to **unsupported-critical-function**. The procedure then terminates.

   NOTE – older implementations may use another value of non-delivery-reason-code which was specified in earlier editions of this Service Definition.

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

4) If the **latest-delivery-time** has passed, or the system's maximum transit time has elapsed for the message's **priority**, the procedure returns a report generation instruction. The **non-delivery-reason-code** is set to **transfer-failure** or **unable-to-transfer** as appropriate and the **non-delivery-diagnostic-code** is set to **maximum-time-expired**. The procedure then terminates.

5) Loop detection is performed. The loop detection algorithm is beyond the scope of this Service Definition. However, an example of a combined routing and loop detection algorithm is given in 14.3.11. If a loop is detected, the procedure returns a report generation instruction. The **non-delivery-reason-code** is set to **transfer-failure** and the **non-delivery-diagnostic-code** is set to **loop-detected**. The procedure then terminates.

6) Depending upon its policy, the MTA may verify that the value of **notification-type** corresponds to the **content**. If the MTA does not verify **notification-type**, or if it corresponds to the **content**, then the procedure terminates successfully. If the MTA verifies **notification-type** and it does not correspond to the **content** then one of the following is performed depending upon policy:

   a) the non-correspondence is ignored and the procedure terminates successfully;

   b) if the **notification-type** is not set to one of the values type-1, type-2, or type-3, **notification-type** is set to the correct value and the procedure terminates;

   c) if the **notification-type** is set incorrectly to one of the values type-1, type-2, or type-3, the procedure returns a report generation instruction with a **non-delivery-reason-code** of **unable-to-transfer** and a **non-delivery-diagnostic-code** of **incorrect-notification-type**. The procedure then terminates.

The MTA may verify **service-message** with similar procedures.

14.3.3 Routing-and-conversion-decision Procedure

For each of a message or probe's recipients for which the MTA is responsible, this procedure determines the routing and conversion actions, if any, to be taken by this MTA. The actions are recorded as per-recipient instructions associated with the message. The actions are subsequently carried out by other sub-procedures within the internal procedure, or elsewhere in the MTA.

NOTE – this procedure may be called multiple times for any particular message. In such cases, the procedure ignores per-recipient instructions generated by previous calls to this procedure which have not yet been acted upon elsewhere.

14.3.3.1 Arguments

1) A message or probe with **responsibility** set to **responsible** for those recipients of concern to this MTA.

14.3.3.2 Results

The message or probe that formed the procedure's argument plus new or revised per-recipient instructions indicating what routing and possible conversion action should be taken by this MTA.

14.3.3.3 Errors

None. Error conditions, if any, are noted in the per-recipient instructions.

14.3.3.4 Procedure Description

Each recipient is considered in turn. If **responsibility** is set to **not-responsible**, the recipient is ignored. Otherwise, the Routing-decision and Conversion-decision procedures are called in turn for this recipient. When all recipients have been considered in this way the procedure terminates. See Figure 9.

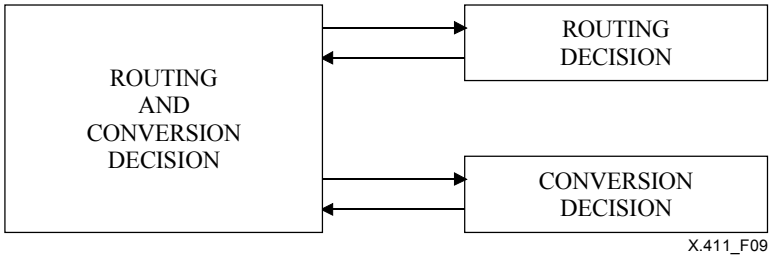


Figure 9 – Organisation of procedures within routing and conversion decision procedure

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

14.3.4 Routing-decision Procedure

This procedure generates a routing instruction for a single message recipient.

14.3.4.1 Arguments

1) A message recipient plus the per-recipient instruction, if any, applicable to this recipient.
2) The per-message instruction, if any, applicable to this message. Other message fields are also accessible to the procedure as required.

14.3.4.2 Results

A new or possibly revised routing instruction applicable to this recipient. Possible instructions are:

a) relay to another MTA;
b) deliver to a local recipient;
c) expand the distribution list represented by this recipient;
d) generate a report indicating delivery failure. The **non-delivery-reason-code** and **non-delivery-diagnostic-code** are included in the instruction;
e) redirect to a preferred address or to a recipient specified alternate recipient.

14.3.4.3 Errors

None. Error conditions are recorded in the routing instruction.

14.3.4.4 Procedure Description

The procedure is described in the following steps.

NOTE – To ensure the security-policy is not violated during routing, the **message-security-label** should be checked as appropriate against the **security-context**.

1) If there is a per-message instruction indicating a previous relay failure, then the procedure attempts to compute an alternate next hop destination for this recipient. The choice of routing algorithm is beyond the scope of this Service Definition. However, an example of an applicable algorithm is contained in 14.3.11. If successful, then the message's **internal-trace-information** is updated with a **rerouted** routing-action to reflect the fact that the message has been re-routed (see 12.3.1). If the message was to have crossed a domain boundary then the **trace-information** is also updated accordingly. The procedure returns a relay instruction to the alternate destination and terminates.

   If no alternate next hop is available or all available next hops have already been tried unsuccessfully or prohibited, then the procedure returns a report generation instruction for this recipient. The **non-delivery-reason-code** is set to **transfer-failure** and the **non-delivery-diagnostic-code** is set as appropriate to the relay failure encountered. The procedure then terminates.

2) If the per-recipient instruction indicates a delivery failure, then the procedure returns a report generation instruction for this recipient. The **non-delivery-reason-code** and **non-delivery-diagnostic-code** are those supplied by the Message-delivery or Probe-delivery-test procedure. The procedure then terminates.

3) If the recipient is specified by an **OR-name** which contains only a **directory-name** (which may happen following distribution list expansion, if a DL member is specified only by **directory-name**), the MTA attempts to acquire the **OR-address** from the Directory. If the **OR-address** cannot be determined, the procedure returns a report generation instruction for this recipient and terminates. The **non-delivery-reason-code** is set to **directory-operation-unsuccessful** and the **non-delivery-diagnostic-code** may be set according to the problem encountered.

   In all other cases than the above, the following steps are taken.

4) If the recipient **OR-address** unambiguously specifies an actual recipient but is not a preferred address of that recipient, then a redirection instruction is generated containing the recipient's preferred **OR-name** and redirection reason **alias**, and the procedure terminates.

5) If the recipient is a distribution list for which this MTA serves as expansion point, then the message's **DL-expansion-prohibited** argument is examined. If the value is **DL-expansion-allowed** then the procedure returns a routing instruction (subject to the security-policy in force) to expand the distribution list and terminates.

   If the value is **DL-expansion-prohibited**, or the security-policy prohibits the use of a DL, then the procedure returns a report generation instruction for this recipient. The **non-delivery-reason-code** is set to **unable-to-transfer** and **non-delivery-diagnostic-code** to **DL-expansion-prohibited**. The procedure then terminates.

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

6) If the recipient **OR-name** identifies a double-envelope-extractor at this MTA and the **content-type** of the message is **inner-envelope**, then the procedure returns a routing instruction to extract the inner envelope from the **content**. The procedure then terminates.

7) If the recipient appears to be local, that is, an MTS-user directly supported by this MTA, then the following steps are taken.

   a) If the **OR-address** does not unambiguously specify an actual recipient the procedure returns a report generation instruction for this recipient. The **non-delivery-reason-code** is set to **unable-to-transfer** and the **non-delivery-diagnostic-code** is set to **unrecognized-OR-name** or **ambiguous-OR-name** as appropriate. The procedure then terminates.

   b) If the **OR-address** unambiguously specifies an actual local recipient, then the recipient registration parameters are checked for **recipient-assigned-redirections**. In the determination of an alternate-recipient the **user-security-label** should be checked against the **message-security-label** to ensure no violation of the security-policy occurs.

      If **recipient-assigned-redirections** has been registered for this recipient, is allowed by the **recipient-reassignment-prohibited** field, and is permitted by the security-policy, then the **encoded-information-types**, **content-length**, **content-type**, **message-security-labels**, **priority**, **originator-name**, **redirection-history** and **DL-expansion-history** of the message are compared with each **redirection-class** from **recipient-assigned-alternate-recipient** in turn until a **redirection-class** is found whose specified values match those of the message. If such a redirection-class is found then the associated **recipient-assigned-alternate-recipient** forms the first argument of a call to the redirection procedure. The other arguments are an indication of the recipient to be replaced, the message, and the redirection-reason **recipient-assigned-alternate-recipient**.

      On normal completion of the redirection procedure the Routing Decision procedure is re-entered. If the redirection procedure signals a redirection loop error then control passes to the error processing procedure.

   c) If **recipient-assigned-redirections** have not caused the message to be redirected, and one or more **deliverable-classes** have been registered, then the MTS determines whether the message satisfies the criteria specified by at least one **deliverable-class**, and so may be delivered.

      For each **deliverable-class**, the message's **encoded-information-types** are compared with the recipient's **encoded-information-types-constraints**, the message's **content-type** is compared with the recipient's **deliverable-content-types**, the message's **content-length** is compared with the recipient's **deliverable-maximum-content-length**, and the message's **security-labels** are compared with the recipient's **deliverable-security-labels**.

      The **encoded-information-types-constraints** component is used together with the **encoded-information-types** specified in the message (the **converted-encoded-information-types** from the last element of trace information which contains this, or the **original-encoded-information-types** otherwise) to decide whether the message may be delivered:

      If no **encoded-information-type** is specified in the message, or the **encoded-information-types-constraints** component is absent, then the message satisfies the **encoded-information-types-constraints** of this deliverable-class.

      Otherwise, if **unacceptable-encoded-information-types** are specified, and the message contains at least one matching **encoded-information-type**, then the message does not satisfy the **encoded-information-types-constraints** of this **deliverable-class**.

      Otherwise, if **acceptable-encoded-information-types** are specified, and the message contains at least one matching **encoded-information-type**, then the message satisfies the **encoded-information-types-constraints** of this **deliverable-class**.

      Otherwise, if **exclusively-acceptable-encoded-information-types** are specified, and the message contains at least one **encoded-information-type** which does not match any in the list, then the message does not satisfy the **encoded-information-types-constraints** of this **deliverable-class**.

      Otherwise, the message satisfies the **encoded-information-types-constraints** of this **deliverable-class**.

      The MTS shall not deliver the message unless it satisfies all the constraints of at least one of the registered **deliverable-classes**.

   d) The **restricted-delivery** registration parameter is used to decide if a message may be delivered:

      If no **restricted-delivery** parameter is registered the message may be delivered.

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

If one or more **restriction** is registered, then the **originator-name**, the **OR-name** from each element of **DL-expansion-history**, and the **OR-name** from each element of **redirection-history** from the message are compared with each registered **restriction** (which has objects set to messages or both) in turn until a match occurs. If delivery is permitted in the matching **restriction** then a delivery instruction is returned, and if not permitted then a report generation instruction is returned.

The procedure to determine an exact-match of **OR-names** is described in the OR-name-match rule in 12.4.4 and pattern-match in the OR-name-elements-match rule in 12.4.5 of ITU-T Rec. X.413 | ISO/IEC 10021-5.

e) If no problem is encountered, then the Routing-decision procedure returns a delivery instruction for this recipient and terminates.

If there is a problem between message and registration parameters, then the procedure returns a report generation instruction for this recipient. The **non-delivery-reason-code** is set to **unable-to-transfer** and the **non-delivery-diagnostic-code** is set as appropriate to the message problem encountered. The procedure then terminates.

7) If the recipient is not local to this MTA, the deliverability considerations in step 6 may be taken into account. If these do not generate an instruction, then the Routing-decision procedure attempts to determine a next hop instruction (subject to the security-policy in force) for this recipient. If successful, then a relay instruction to the next hop is returned and the procedure terminates.

If the security-policy specifies that a double envelope is required for the identified next hop and the **content-type** of the message is not **inner-envelope**, then the procedure returns a routing instruction to embed the current message within the **content** of a new message using the procedure specified in 14.3.13. The procedure then terminates.

If a next hop cannot be determined, then the procedure returns a report generation instruction for this recipient. The **non-delivery-reason-code** is set to **unable-to-transfer** and the **non-delivery-diagnostic-code** is set as appropriate to the problem encountered. The procedure then terminates.

14.3.5 Conversion-decision Procedure

This procedure generates a conversion instruction for a single message recipient.

14.3.5.1 Arguments

1) A message or probe recipient plus the per-recipient instruction, if any, applicable to this recipient.
2) Other message fields are also considered by the procedure:
   a) the current **encoded-information-types**, given by the latest **converted-encoded-information-types** in **trace-information**, if such a field exists, or else by **original-encoded-information-types**,
   b) **implicit-conversion-prohibited**,
   c) **conversion-with-loss-prohibited**,
   d) **explicit-conversion**.

14.3.5.2 Results

1) A content conversion instruction applicable to this recipient,

and, possibly:

2) A revised routing instruction indicating Relay-out or Probe-out to an MTA able to perform the required conversion,

or, in lieu of 1 and 2 above:

3) An instruction to generate a report indicating delivery failure. The **non-delivery-reason-code** and **non-delivery-diagnostic-code** are included in the instruction.

14.3.5.3 Errors

None. Error conditions are recorded in the routing instruction.

14.3.5.4 Procedure Description

NOTE – As the circumstances under which a particular MTA stages conversion may be the subject of future standardization, it is impractical to describe a procedure to decide what EITs are required for conversion output. For example, if an intermediate MTA stages the conversion, there is no standardized way to know the EITs that the MTS-user can handle. Consequently the following clauses assume that the EITs for conversion are known to the MTA.

1) If explicit conversion is required for this recipient, the procedure starts at step 6.

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

2) If implicit conversion is required but the recipient has not subscribed to the implicit conversion facility, the procedure returns a negative report instruction with the **non-delivery-reason-code conversion-not-performed** and the **non-delivery-diagnostic-code implicit-conversion-not-subscribed**. The procedure then terminates.

3) If the required conversion is impractical, the procedure generates a negative report instruction with the **non-delivery-reason-code conversion-not-performed** and the **non-delivery-diagnostic-code conversion-impractical**. The procedure then terminates.

4) If conversion would be required but is prohibited for the message, the procedure generates a negative report instruction with the **non-delivery-reason-code conversion-not-performed** and the **non-delivery-diagnostic-code conversion-prohibited**. The procedure then terminates.

5) If the required conversion would cause a loss of information and the **conversion-with-loss-prohibited** field has the value **with-loss-prohibited**, the procedure generates a negative report instruction with the **non-delivery-reason-code conversion-not-performed** and one of the following **non-delivery-diagnostic-codes**, as appropriate:

   line-too-long,
   page-split,
   pictorial-symbol-loss,
   punctuation-symbol-loss,
   alphabetical-character-loss, or
   multiple-information-loss.

   The procedure then terminates.

6) If the required conversion cannot be performed by this MTA, and it is known that another MTA can perform it, then no conversion instruction is generated. The routing instruction previously generated is changed to Transfer-out or Probe-out, with a next hop destination appropriate to the MTA in question. Care should be taken, however, to avoid a routing loop. The procedure then terminates.

7) If the required conversion can be performed by this MTA, the procedure returns an instruction to perform the conversion and terminates.

14.3.6 Error-processing Procedure

When another procedure encounters a deliverability or routing error, this procedure is called to determine whether delivery or routing can be achieved by reassignment of the recipient or by choosing a different **OR-address** for the same recipient. If not, non-delivery must be signalled to the Report module. Errors provoking a call on this procedure include:

- **recipient-name** does not identify an MTS-user or DL;
- delivery failure;
- MTA is unable to perform necessary conversion;
- transfer path problems;
- DL-expansion problems;
- security violations;
- conflict with registration parameters.

NOTE – The action taken on Error-processing shall be subject to the security-policy in force.

14.3.6.1 Arguments

1) A message or probe with the per-recipient fields that caused the problem.
2) Report instructions indicating the error.

14.3.6.2 Results

The message or probe in question with an updated **recipient-name** field,

or

1) The message or probe in question.
2) Report instructions.

14.3.6.3 Errors

None.

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

14.3.6.4 Procedure Description

NOTE – This procedure may be called multiple times for a given recipient. Eventually all alternatives will be exhausted and step 5 executed to report failure.

1) The arguments are checked for the inclusion of a **directory-name**. If one is present, the Directory Name Resolution procedure (see 14.3.12) is called to determine a new **OR-address**. If this is different from the original **OR-address**, it is combined with the **directory-name** to form the **OR-name** of an alternate recipient. The Redirection procedure is then called to redirect the message to this alternate recipient, with redirection-reason **directory-look-up**.

2) Otherwise the procedure determines whether an **originator-requested-alternate-recipient** was specified for the recipient of concern. If so and if it is different from the current **recipient-name**, the Redirection procedure is called with the message, relevant fields indicated, as argument. Upon successful return from Redirection, the procedure terminates, returning the now redirected message as result.

3) Otherwise the procedure checks for a delivery error, and if present checks the error's cause by examination of the **non-delivery-reason-code** and **non-delivery-diagnostic-code**. If the recipient **OR-address** does not identify an MTS-user or DL, then the **per-message-indicators** are checked for **alternate-recipient-allowed**. If the value found is **alternate-recipient-allowed**, and the MTA has been configured with an alternate-recipient for this class of recipient which is different from the current **recipient-name**, then Redirection is called to redirect the message to the alternate-recipient. Upon successful return from Redirection, the procedure terminates, returning the now redirected message as result.

4) The handling of errors which can be resolved but are due to other than addressing problems is a local matter, for example routing to another MTA within the domain because of conversion problems.

5) If the delivery error is of a type other than those cited above, or if the value of **alternate-recipient-allowed** is **alternate-recipient-prohibited**, or if no suitable MD-specified alternate-recipient exists, then the procedure returns a report instruction and terminates.

14.3.7 Redirection Procedure

This procedure redirects a message.

NOTE – The use of redirection facilities shall be subject to the security-policy in force.

14.3.7.1 Arguments

1) The **OR-name** of the replacement recipient to whom the message is to be redirected.

2) The per-recipient message fields for the recipient to be replaced by an alternate.

3) The message or probe which is to be redirected.

4) The redirection reason.

14.3.7.2 Results

The message or probe supplied in the third argument with the recipient identified in the second argument replaced by the replacement recipient specified in the first argument.

14.3.7.3 Errors

An indication that a redirection loop has been detected.

14.3.7.4 Procedure Description

1) The procedure first ensures that redirection to the specified replacement recipient would not result in a redirection loop. The **OR-address** of the replacement recipient supplied in argument 1 is compared with each **intended-recipient-name** from the sequence of **redirection-history** from the per-recipient fields identified in argument 2. Upon a match the procedure terminates indicating that a redirection loop has been detected.

2) An element is appended to the **redirection-history** (which is created if not present), using the **recipient-name** from argument 2 to form the **intended-recipient-name**, obtaining the **redirection-reason** from argument 4, and containing the time at which this redirection is performed. The **OR-name** supplied in the first argument is then substituted for that **recipient-name**.

3) In the **other-actions** field of the current **trace-information** and **internal-trace-information**, if **dl-operation** is not already indicated then the value **redirected** is indicated, otherwise new **trace-information** and **internal-trace-information** elements are created with the value **redirected** indicated.

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

4) The message transfer envelope is updated as follows:

recipient-name:	replaced
trace-information/internal-trace-information	indicate **redirected**
redirection-history:	append previous **recipient-name** and **redirection-reason**
originator-requested-alternate-recipient:	deleted if, and only if, **redirection-reason** indicates **originator-requested-alternate-recipient**.

14.3.8 Splitter Procedure

The Splitter replicates messages and probes as required for further processing. The replicas are modified as appropriate to correctly indicate the distribution of **responsibility** for the various recipients from the original. Each replica is accompanied by a per-message instruction indicating its further disposition within the MTA.

NOTE – The use of Splitter facilities shall be subject to the security-policy in force.

14.3.8.1 Arguments

A message or probe. For each recipient with **responsibility** set to **responsible** a per-recipient routing/conversion instruction accompanies the message.

14.3.8.2 Results

One or more replicas of the original message or probe with **responsibility** appropriately indicated, and a per-message instruction indicating the replica's further disposition within the MTA.

14.3.8.3 Errors

None.

14.3.8.4 Procedure Description

The Splitter examines the instructions generated by the Routing-and-conversion-decision procedure to (conceptually) segregate the recipients with **responsibility** set to **responsible** into groups. A replica is created for each group. Further processing for that replica (in other procedures) is dependent on the routing and conversion instructions applicable to the group it represents.

NOTE 1 – Message replication is required in an MTA because of the potentially differing treatment required for a message's various recipients. These differences arise from the need for more than one relaying path outward from an MTA, from the need for more than one conversion to be carried out on the message's content and from the need to expand distribution lists. For example when more than one relay path exists, a separate copy of the message must be created for each such path, with **responsibility** values as appropriate for the recipients lying along that path.

NOTE 2 – The determination of what replicas are needed is a local matter, undertaken to minimize the total number of such replicas created. The following paragraphs suggest one approach but are not intended to constrain in any way the approach followed in an actual implementation.

NOTE 3 – For simplicity of exposition, the Splitter is described as a single-pass algorithm. That is, all necessary replicas are created prior to any further processing. An important optimisation would be to minimally split the message for conversion, and then to complete the splitting of the converted copies.

1) The procedure considers first those recipients for which content conversion instructions exist. These recipients are grouped such that the members of each group are subject to identical conversion instructions. A replica is created for each such group with **responsibility** set to **responsible** for the recipients in that group, **not-responsible** for all others.

2) The recipients are then examined for those for which DL-expansion instructions exist. A replica is created for each such DL recipient with **responsibility** set to **not-responsible** for all recipients but the single DL that yielded the replica.

3) The groups are further subdivided based on per-recipient routing instruction calls for Transfer-out or Probe-out. These recipients are grouped such that each group shares a common next hop destination. A replica is created for each such group with **responsibility** set to **responsible** for recipients in the group, **not-responsible** for all others. For all recipients in each such group, this will be either the first relay attempt or a re-routing attempt. In the latter case the trace-information for the message or probe is modified to indicate that this is a first or subsequent re-routing.

4) Finally, the routing instructions for some recipients will call for Message-delivery or Report-generation. A replica is created for each such subgroup with **responsibility** set to **responsible** for the recipients in the group, **not-responsible** for all others.

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

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

5) If **disclosure-of-other-recipients** is not requested, recipients whose **responsibility** is set to **not-responsible** may be removed.

6) Any per-recipient-extensions for those recipients with **responsibility** set to **not-responsible** may be deleted.

7) The procedure now terminates.

14.3.9 Conversion-procedure

This procedure performs conversions on messages and indicates those conversions that would have been performed on probes.

14.3.9.1 Arguments

A message or probe with the required conversion(s) indicated.

14.3.9.2 Results

The message or probe with conversions performed and indicated (just indicated in the case of a probe).

14.3.9.3 Errors

The message or probe with report instructions detailing the conversion problem encountered.

14.3.9.4 Procedure Description

1) For a message, the conversion procedures for built in EITs are performed as defined in CCITT Rec. X.408. The conversion procedures between externally defined EITs and between built in and externally defined EITs are outside the scope of this Service Definition.

2) Upon conversion the message or probe's **trace-information** for this domain and **internal-trace-information** for this MTA is updated to show the converted EITs. The procedure now terminates.

14.3.10 Distribution-list-expansion Procedure

This procedure takes a message with a single DL recipient and returns a message who's recipient list includes the members of the DL. For a probe it verifies whether DL-expansion would occur, if requested.

NOTE – The use of DL-expansion shall be subject to the security-policy in force.

14.3.10.1 Arguments

1) A message with information indicating the recipient DL which is to be expanded, or

2) A probe with information indicating the recipient DL who's expansion is to be verified.

14.3.10.2 Results

1) The message with zero or more recipients representing the DL's membership. Other fields can be updated as indicated in the procedure description below.

2) Optionally, the message with report generation instructions to indicate successful delivery.

or

3) The probe with a report generation instruction.

14.3.10.3 Errors

1) A report instruction indicating delivery failure. Values for the **non-delivery-reason-code** and **non-delivery-diagnostic-code** are as indicated in the procedure description below.

2) In the case of DL recursion the procedure terminates without returning errors or results.

14.3.10.4 Procedure Description

1) For a message (not a probe), do Recursion Detection: The components of the **DL-expansion-history** field are examined for an occurrence of the DL recipient's name. DL expansion is performed either by use of an entry stored in the Directory, or by local configuration of the DL's membership. Where the DL is expanded by use of the Directory, the distinguished **directory-name** of the DL, following de-referencing of any aliases, shall be compared with the **directory-name** from each **OR-name** in the **DL-expansion-history**, and the **OR-addresses** shall be ignored. Where the DL is expanded by use of local configuration, each MTA capable of expanding the DL must be aware of all the **OR-addresses** that the DL has, and recursion detection shall be performed by comparison of **OR-addresses**.

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

If the DL recipients name is present in the **DL-expansion-history**, then the DL is recursively defined and shall not be expanded further. The message is discarded and no reports or other results are returned. The expansion procedure terminates.

2) DL acquisition: The expansion procedure attempts to acquire the DL attributes.

   If unsuccessful the procedure returns a report instruction with the **non-delivery-reason-code unable-to-transfer** and **non-delivery-diagnostic-code** as appropriate. The procedure then terminates.

3) Submit permission verification: If it is a message (not a Probe), the last element of the **DL-expansion-history** field (if present) else the **originator-name** is considered to be the sender of the message. For a probe the originator is the sender of the message.

   The sender's name is compared against the components of the DL-submit-permission. If no match, return a report instruction with the **non-delivery-reason-code unable-to-transfer** and **non-delivery-diagnostic-code no-DL-submit-permission**. The procedure then terminates.

4) For a probe: If no other local policy would prevent an attempted delivery, then return a report instruction for successful delivery indication. Procedure then terminates.

5) For a message: The DL recipient's **responsibility** flag is set to **not-responsible**. If the MTA performing DL expansion supports the **DL-exempted-recipients** argument, the members of the DL are then compared with the values of this argument. If any value of the **DL-exempted-recipients** argument lacks an **OR-address** component, then this is obtained from the MHS OR-Addresses attribute from that argument's Directory entry. If multiple OR-addresses are present in that Directory attribute, then each value is incorporated in the argument. The **OR-address** and the **directory-name** components of the DL-exempted-recipients attribute are compared for equality with the **OR-address** or **directory-name** values (using the **OR-name-match** rule described in 12.4.4 of ITU-T Rec. X.413 | ISO/IEC 10021-5) for each member of the DL. If either the **OR-address** or **directory-name** component matches a DL member, then that member shall not be added as a new recipient of the message. The **DL-exempted-recipients** argument shall be retained unchanged in the envelope regardless of how many elements were successfully matched to DL members. All DL's members not matching a value of **DL-exempted-recipients** shall be added as new recipients of the message. The per-recipient fields for each new recipient are copied from those of the DL recipient, except as follows:

   recipient-name: member of the DL.

   The following per-recipient fields are copied or changed according to local DL policy:

   originating-MTA-report-request (**see Note 1**),
   originator-report-request (**see Note 1**),
   originator-requested-alternate-recipient (**see Note 2**),
   explicit-conversion,
   proof-of-delivery-request (**see Note 4**),
   requested-delivery-method.
   message-token (**see Note 6**)
   body-part-encryption-token (**see Note 6**)
   forwarded-content-token (**see Note 6**)

   NOTE 1 – Must be copied and must not be changed if DL-policy is to pass reports back; may be changed as required if DL-policy is not to pass reports back.

   NOTE 2 – The **originator-requested-alternate-recipient** can be removed or replaced, according to local DL policy, or copied, but only if explicitly required by DL-policy.

   NOTE 3 – Any DL-members that identify DLs that are already present in the **DL-expansion-history** may be excluded from the DL expansion and not included in the new recipients of the message.

   NOTE 4 – Whether **proof-of-delivery-request** produces a **proof-of-delivery** from the DL expansion point, or from the DL members, or from both, or from neither, depends on the DL policy and on the security policy in force.

   NOTE 5 – Where a DL member is identified only by a directory name, the necessary processing to obtain an **OR-address** is described in the routing decision procedure.

   NOTE 6 – When a message is expanded which contains encrypted data in a token for the DL recipient, then that encrypted data is decrypted using the private key of the DL and a new token is created for each member recipient with the decrypted data re-encrypted using the first algorithm in the token-encryption-algorithm-preference which is supported by both the DL expanding MTA and by that DL member, and the new token signed using the first algorithm in the token-signature-algorithm-preference which is supported by both the DL expanding MTA and by that DL member.

6) In the **other-actions** field of the current **trace-information** and **internal-trace-information**, if **redirected** is not already indicated then the value **dl-operation** is indicated, otherwise new **trace-information** and **internal-trace-information** elements are created with the value **dl-operation** indicated.

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

7) The value of the **recipient-name** of the DL recipient (which shall include its distinguished **directory-name**, following de-referencing of any aliases, if it has one) and the time at which this expansion occurred are appended to the **DL-expansion-history** field of the message.

NOTE – The current value of the **recipient-name** will be a preferred value, as a result of actions specified in 14.3.4.4 bullet 3).

8) If the new report request values (determined in step 5) or the DL's local policy will prevent the originator receiving a requested delivery report from the DL's members, then a copy of the message, with delivery report request instructions for the expanded DL, is constructed and returned along with the message.

In this case (where the DL policy will not send reports from DL members to the originator), if any DL member has associated with it the DL-reset-originator Context (see ITU-T Rec. X.402 | ISO/IEC 10021-2), then a procedure akin to the Splitter procedure is used to make two copies of the message: one copy for members without the DL-reset-originator Context, and the other for members with the DL-reset-originator Context. In the copy for members with the DL-reset-originator Context, the originator-name field is changed to the OR-name of the DL's owner.

9) The procedure returns the revised message and the optional report request and then terminates.

14.3.11 Loop Detection and Routing Algorithm

The routing and loop detection algorithms for inter or intra domain use are beyond the scope of this Service Definition. In order to expose the issues that must be considered, the remainder of this clause describes one approach toward routing and loop detection. This material is informative.

The paragraphs that follow describe a simple method of loop detection together with a minimal routing algorithm The algorithm is minimal in the sense that it presupposes only minimal knowledge from each MD and performs transfer steps that avoid loops (in the sense indicated below). Of course, this algorithm can be improved any time an MD knows more about the topology of the network of MDs.

The algorithm recognizes the fact that it is in general legitimate (i.e. no loop should be detected) to re-enter an MD if a specific operation has been performed by another MD since the last passage through the MD about to be re-entered. Legitimate operations are: conversion, DL-expansion, and redirection.

1) Notation: The Trace Information sequence is made of **trace-information-elements** denoted in a simplified way as [MD, routing-action, operation], where MD is the name of an MD; routing-action is 'relayed' or 're-routed', operation is 'conversion', 'DL-operation', 'redirection' or 'nil'. M denotes the message to transfer. MD(o) denotes the current MD (the one currently doing loop detection). Neighbours is the set of selected adjacent MDs (neighbours of MD(o)), which are possible relay-MDs for M. Trace-Info* is the sequence of Trace-Info obtained by considering the tail of the trace info sequence beginning with the last [MD, r, op] trace info element where op is not nil (nil indicates that no operation has been performed by an MD).

2) Loop Detection: Examine Trace-Info for loops. A loop is detected if the trace info sequence contains a trailing sub-sequence, [MD(o), relayed, op(o)] ... [MD(p), relayed, op(p)] where for all j for which o < j </= p the associated trace info element is [MD(j), relayed, op(j)] and op(j) = nil. That is, a loop is detected if M arrives at an MD which has already relayed it and each MD afterwards has also relayed it without performing any operation other than routing. If a loop is detected, then the algorithm returns an error indicating the problem, and terminates.

3) Routing Set-up: If no loop is detected, the set, Neighbours, is adjusted, if necessary, for loop-avoiding transfer steps in the context of the current message. (The adjustment affects no other message).

   a) If there is no loop and no occurrence of [MD(o), r, op] in Trace-Info*, then Neighbours is unchanged.

   b) If there is no loop but there is an occurrence of [MD(o), r, op] in Trace-Info*, then remove from Neighbours all MDs which appear in that suffix of Trace-Info* which begins with [MD(o), r, op]. Modify the trace info element added by the current domain to show re-routed as routing action. Add a previous-MD parameter determined as follows: The last [MD(o), r, op] trace info element in Trace Info is located. The previous-MD is the MD appearing in the first trace info element after this last [MD(o), r, op] trace info element.

   c) In cases a and b, if Neighbours is empty, the algorithm returns an error indicating the problem and terminates.

4) Routing action. A next hop is selected from Neighbours for each recipient to be relayed.

14.3.12 Directory Name Resolution Procedure

This procedure obtains an **OR-address** for a user identified by a Directory Name

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

14.3.12.1 Arguments

The Directory Name of the user, the originator's **requested-delivery-method** if specified, and the **redirection-history** if present.

14.3.12.2 Results

An **OR-address** of the user

14.3.12.3 Errors

An indication that the directory name could not be resolved.

14.3.12.4 Procedure Description

1) The MTA accesses the Directory, using the supplied Directory Name. If the Name does not identify a Directory entry, the procedure returns an error and terminates.
2) If the **requested-delivery-method** argument is not supplied, or is **any-delivery-method**, the MTA attempts to obtain the *preferred-delivery-method* attribute from the Directory entry. If the remaining steps allow the construction of more than one type of address, the choice between them is based on a combination of the **requested-delivery-method** (or *preferred-delivery-method*) and local policy. If a choice between **OR-addresses** is to be made and a **redirection-history** argument exists, then any **OR-address** which is already present in the **redirection-history** is excluded before making the choice.
3) If the *mhs-or-addresses* attribute is present, a value of this attribute may be returned. Such a value is considered to satisfy a request for the **mhs-delivery** method. If multiple attribute values are present, the choice between them is a local matter. The choice may be influenced by the recipient's UA's capabilities (determined from other Directory attributes or local knowledge) and the characteristics of the message.
4) The MTA may be configured with information about various Access Units which it is permitted to use when constructing an **OR-address** from information supplied by the Directory. The configured information will include **OR-address** attribute values, which may be combined with information retrieved from the Directory to form a complete **OR-address**, and the delivery method implied by such an address. If the MTA is configured with details of more than one access unit of the same type, the choice between them is subject to local policy. The MTA may be configured with information concerning zero or more of the following types of Access Unit:
   a) physical-delivery: Values of **country-name**, **administration-domain-name**, optionally **private-domain-name**, and **pds-name** are configured. The **OR-address** is constructed from the configured components, values of **unformatted-postal-address** and **postal-code** obtained from the *postalAddress* and *postalCode* Directory attributes, and **physical-delivery-country-name** derived from the *countryName* component of the Directory entry's Distinguished Name. This is considered to satisfy the **physical-delivery** method.
   b) g3-facsimile-delivery: Values of **country-name**, **administration-domain-name**, and optionally **private-domain-name** are configured. The **OR-address** is constructed from the configured components and a **network-address** obtained from the value of the *facsimileTelephoneNumber* Directory attribute, and **terminal-type** set to the value *g3-facsimile*. This is considered to satisfy the **g3-facsimile-delivery** method.
   c) telex-delivery: Values of **country-name**, **administration-domain-name**, and optionally **private-domain-name** are configured. The **OR-address** is constructed from the configured components and a **network-address** obtained from the values of the telexNumber and countryCode components of the *telexNumber* Directory attribute, a **terminal-identifier** obtained from the value of the answerback component of the *telexNumber* Directory attribute, and **terminal-type** set to the value *telex*. This is considered to satisfy the **telex-delivery** method.

14.3.13 Double-enveloper Procedure

This procedure takes a message, probe or report, and places the entire object in the content of a new message which is addressed to a remote double-envelope-extractor, and submitted as a new message which has an **inner-envelope content-type**.

14.3.13.1 Arguments

1) A message, probe or report which is to be wrapped in an outer-envelope.
2) The **OR-name** of the remote double-envelope-extractor.
3) The **OR-name** of this double-enveloper.

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

4) The security services to be applied to protect the inner-envelope content and either specific algorithm information or algorithm preferences for these (for content-confidentiality, message-token-encrypted-data, message-token-signed-data, and message-origin-authentication-check).

14.3.13.2 Results

None, as the MTA has no further processing to perform on the original message.

NOTE – There are two output events from this procedure: one is submission of a new message containing the inner-envelope, and the second is a record of sufficient information to enable the double-enveloper to construct a non-delivery report on the original message in the event that it receives a non-delivery report on the new message.

14.3.13.3 Errors

An indication of a security-error if a requested service could not be provided.

NOTE – The occurrence of such a security-error may indicate a configuration error (where a configured algorithm, or the MTA's private-key for it, is unavailable), or an error in the certificate of the double envelope extractor.

14.3.13.4 Procedure Description

The entire MTS-APDU containing the subject message, probe or report, is placed in the content of a new message, whose originator is the **OR-name** of this double-enveloper and whose recipient is the **OR-name** of the remote double-envelope-extractor. The originator-report-request for this recipient is set to report, and the content-type is set to inner-envelope.

If algorithm preferences are specified for the requested security services and the directory-name is present within the **OR-name** of the remote double-envelope-extractor, then that Directory entry is read to obtain its Supported Algorithms and User Certificate attribute. The algorithm highest in the preference order which is supported by both this MTA and by the remote double-envelope-extractor is selected for each requested security service (i.e. content-confidentiality, message-token-encrypted-data, message-token-signed-data, and message-origin-authentication-check). The algorithm-information contains an algorithm-identifier, and, optionally, information to select an appropriate Certificate for that algorithm for the originator or recipient or both (depending on the requirements of the algorithm). Certificate-selector information is required only if the Directory entry may contain more than one Certificate for the identified algorithm. If the directory-name is not present, then the highest preference is selected, and local configuration of the remote double-envelope-extractor's public encryption key will be required.

The content is encrypted using the selected (or configured) content-confidentiality-algorithm which may be an asymmetric algorithm, or if this is a symmetric algorithm then a random content-confidentiality-key is generated and used to encrypt the content, and a message-token created with this key encrypted using the selected (or configured) message-token-encryption-algorithm (which must be an asymmetric algorithm) and signed using the selected (or configured) message-token-signature-algorithm (which must be a signature algorithm). The public key that is used with the asymmetric encryption algorithm is found by using the algorithm-identifier and recipient-certificate-selector to select an appropriate Certificate from the Directory entry.

If message-origin-authentication is specified, then a message-origin-authentication-check is computed containing a signature of the encrypted content using the selected (or configured) algorithm together with the private key of this MTA corresponding to its Certificate identified by originator-certificate-selector.

The new message containing the inner-envelope is submitted, and a record is made of its message-submission-identifier together with sufficient information to enable the double-enveloper to construct a non-delivery report on the original message in the event that it receives a non-delivery report on the new message.

14.3.14 Double-envelope-extractor Procedure

This procedure takes a message which has an inner-envelope content-type and extracts from its content a message, probe or report which the MTA then processes as if it had been transferred normally.

14.3.14.1 Arguments

A message which has an inner-envelope content-type.

14.3.14.2 Results

A message, probe or report.

14.3.14.3 Errors

An indication of a security-error if verification of a security argument failed.

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

In response to a probe, or to a message with a content-type other than inner-envelope, a report generation instruction unable-to-transfer unrecognised-OR-name.

14.3.14.4 Procedure Description

The message-delivery procedure (see 14.7.1) is followed (as appropriate), including generation of a report instruction where requested.

If message-origin-authentication-check is present, then this is verified. The content is decrypted, and the message, probe or report is extracted and passed to the front-end (or report-front-end) procedure.

14.4 Report Module

The Report module can be invoked by:

1) the Report-in module, which passes a report, or
2) the Main module, which passes a message or probe with report instructions, or
3) the Report-out module, which passes a report with failure description.

If an error is encountered by the procedures internal to this module, no output is generated. Otherwise the Report module invokes the Report-out or Report-delivery module, passing a report with transfer or delivery instructions, respectively. See Figure 10.

NOTE – The use of reports shall be subject to the security-policy in force.

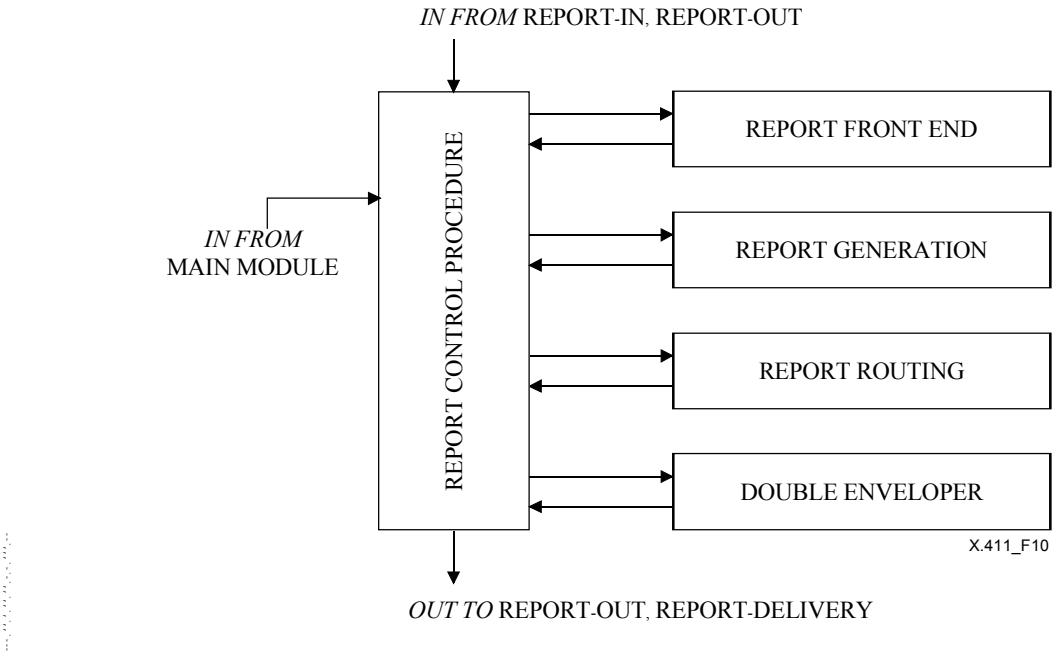


Figure 10 – Organisation of Procedure within the Report Module

14.4.1 Control Procedure

14.4.1.1 Arguments

1) A report or,
2) A message or probe with report instructions.

14.4.1.2 Results

1) A report with relaying or delivery instructions or
2) No result in case an error is encountered.

14.4.1.3 Errors

None. The report, message, or probe is discarded if an error is encountered.

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

14.4.1.4 Procedure Description

1) For a report from Report-in the Report-front-end procedure is first called to perform trace initialisation and several initial verification steps. A null return indicates an error; the report is discarded and processing terminates. Otherwise processing continues at step 3 below.
2) For a message or probe the Report-generation procedure is first called to create a report. A null return indicates an error; the message or probe is discarded and processing terminates. If a report is returned, processing continues at step 3, below.
3) The Report-routing procedure is called to generate a routing instruction for the report. A null return indicates an error; the report is discarded and processing terminates. The Control procedure returns the completed report together with routing instruction and terminates, subject to the security-policy.

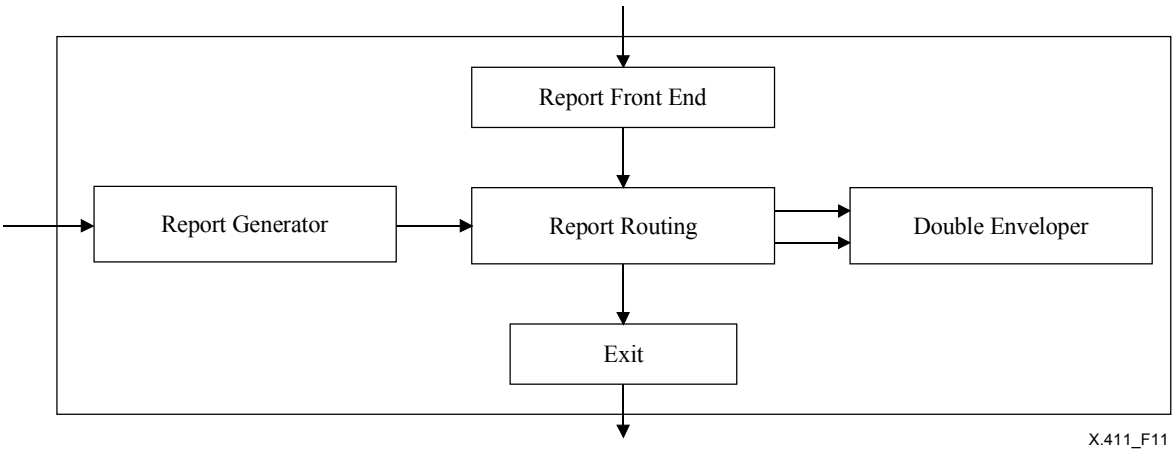


Figure 11 – Information Flow within the Report Module

14.4.2 Report-front-end Procedure

This procedure performs trace initialisation, detection of message-expiration violations, initial security check, loop detection and criticality check.

14.4.2.1 Arguments

A report.

14.4.2.2 Results

The report with initialised **trace-information** for this MTA.

14.4.2.3 Errors

None. The report is discarded if an error is detected.

14.4.2.4 Procedure Description

1) If the report has crossed a domain boundary, a **trace-information-element** for this domain is added with current time as the **arrival-time** and **relay** as **action**. An **internal-trace-information-element** is also added whether or not the report has crossed a domain boundary.
2) If required by the security-policy in force and/or if the **report-origin-authentication-check** is incorrect, the report is discarded and processing terminates.
3) If any of the extension fields is marked critical for transfer but is not semantically understood by the MTA, the report is discarded. The procedure then terminates.
4) Loop detection is performed. The loop detection algorithm is beyond the scope of this Service Definition. However, an example of a combined routing and loop detection algorithm is given in 14.3.11. If a loop is detected, the report is discarded and the procedure terminates.

14.4.3 Report-generation Procedure

This procedure generates a report describing the success and/or failure of operations attempted by this MTA.

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

14.4.3.1 Arguments

A message or probe. For each recipient with **responsibility** set to **responsible**, a per-recipient instruction is included indicating the success or problem to be reported.

14.4.3.2 Results

A report describing the successes or failures to be reported.

14.4.3.3 Errors

None.

14.4.3.4 Procedure Description

If the subject's **originating-MTA-report-request** field so indicates, the report is constructed with arguments as described in Table 32, and further amplified by the following:

The Delivery arguments (**message-delivery-time**, **type-of-MTS-user**) or Non-delivery arguments (**non-delivery-reason-code**, **non-delivery-diagnostic-code**) for each recipient are taken from the per-recipient instructions that accompanied the subject message. If successful delivery is reported for a DL recipient, then the **type-of-MTS-user** is set to **DL**. The **report-destination-name** is the last element from **DL-expansion-history**, if that element exists. For messages with no **DL-expansion-history** and for all probes, the **report-destination-name** is the subject's **originator-name**. The **originator-and-DL-expansion** will contain the **originator-name** and the subject's **message-submission-time** followed by the content of **DL-expansion-history**. A **trace-information-element** for this domain is created with the current time as the **arrival-time** and **relay** as **action**. An **internal-trace-information-element** is also created. If the subject contains a **redirection-history** or a **dl-expansion-history** then the **originally-intended-recipient-name** shall be copied from the first element of either the **redirection-history** or the **dl-expansion-history**, whichever event occurred first (and the sequence of these events shall be determined from the **trace-information**).

NOTE – **reporting-DL-name** is not generated under any of these conditions.

In the case where the instructions reflect multiple failures, the report should reflect the original problem rather than the failure of subsequent recovery actions.

The MTA nominates **criticality** values for fields copied from the subject. These new values reflect criticality with regard to the report, not the subject. The MTA will not copy into the report any critical functions which it does not support.

14.4.4 Report-routing Procedure

This procedure determines the routing action, if any, to be taken on a report. Report-routing reflects special conditions that require a routing procedure different from that applicable to messages or probes:

1) A report has just one recipient – the originator of the message that forms the subject of the report, a DL expansion-point, or, if local policy allows, a DL owner.
2) Insurmountable failures encountered in routing a report result in the discarding of the report. No attempt is made to generate a further report on the difficulty encountered.

The processing actions necessitated by these conditions are described in the following clauses. It should be noted that the routing of reports is subject to the security-policy.

14.4.4.1 Arguments

One of the following:

1) A report transferred to this MTA from another MTA and successfully processed by the Report-front-end procedure.
2) A report created by the Report-generation procedure internal to this MTA.
3) A report received back from the Report-out procedure together with a description of the transfer failure encountered.

14.4.4.2 Results

One of the following:

1) The report, together with relaying instructions to the next hop MTA.
2) The report, together with an indication of the locally supported MTS-user who is to receive Report-delivery.

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

14.4.4.3 Errors

None. If no local recipient or next hop can be determined, the report is discarded.

14.4.4.4 Procedure Description

1) Reports relayed to this MTA or generated locally receive normal routing attention as follows:

   a) If the Report-destination is not local to this MTA then relaying is required. Report-routing attempts to determine the next hop address. In this determination the **message-security-label** of the report is checked against the **security-context** to ensure no violation of the security-policy occurs. If successful, then the report, together with this information is returned as the procedure's result. The procedure then terminates. The report is subsequently passed to the Report-out procedure.

      If the security-policy specifies that a double envelope is required for the identified next hop, then the procedure returns an instruction to embed the report within the **content** of a new message using the procedure specified in 14.3.13. The procedure then terminates.

      If the next hop address cannot be determined, then the report is discarded and the procedure terminates without returning a result.

   b) If the Report-destination unambiguously specifies an actual recipient but is not a preferred address of that recipient, then a redirection instruction is generated containing the recipient's preferred **OR-name** and redirection reason **alias**, and the procedure terminates.

      If the Report-destination unambiguously specifies an actual local recipient, then the recipient registration parameters are checked for **recipient-assigned-redirections**. If this is in effect then the length of the returned-content, if any, is compared with the **content-length** and the content-type, if present, with the **content-type** of each **redirection-class** (which has objects set to reports or both) from **recipient-assigned-redirections** in turn until a **redirection-class** is found whose specified values for these fields match those of the report. Values specified for other components of **redirection-class** are ignored. If a **redirection-class** matches then a redirection instruction is generated and the procedure terminates.

   c) If the Report-destination is an MTS-user local to this MTA, and the **originator-report-request** field indicates, then Report-delivery is required (subject to the security-policy in force). Report-routing attempts to determine the OR-address of the report destination. If successful, then the report, together with this information is returned as the procedure's result. The procedure then terminates. The report is subsequently passed to the Report-delivery procedure.

      If the Report-destination does not identify an MTS-user and the MTA has been configured with the address of an alternate-recipient for this class of Report-destination, then a redirection instruction is generated with redirection reason recipient-MD-assigned-alternate-recipient, and the procedure terminates.

      If the report was not requested or the report destination address cannot be determined, the report is discarded and the procedure terminates without returning a result.

   d) If the **report-destination-name** is of a DL local to this MTA, then this report is in process of routing back along a path of successive DL expansion-points. In the **other-actions** field of the current **trace-information-element** and **internal-trace-information-element**, the value **dl-operation** is indicated.

      Any processing based on local DL policy would occur here; e.g. a copy of the report can be constructed and sent to the DL owner. In this case the **report-destination-name** will be that of the DL owner and the **reporting-DL-name** will be constructed to contain the subject DL name. This copy of the report shall not contain the **returned-content**. In addition, suppression of reports can be done here.

      NOTE 1 – The possibility that a DL owner is itself a DL may be the subject of future standardization.

      NOTE 2 – DL-submit-permission is not considered when processing a report.

      If the report is not to be suppressed, the MTA then replaces the **OR-name** currently in the **report-destination-name** field by the **OR-name** immediately preceding that one in the **originator-and-DL-expansion-history** field. Thus the report acquires, as a new destination, the next entry back along the chain of entries in the **originator-and-DL-expansion-history** field:

report-destination-name:	Copy previous DL **OR-name** from **originator-and-DL-expansion-history**.
reporting-DL-name:	Generated only in case of reports to DL owner.

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

In order to route the report to this new destination, the Report-routing procedure now calls itself recursively. The result returned, if any, from this recursive call is returned, and the procedure terminates.

e) If the **report-destination-name** identifies a double-enveloper at this MTA, then the procedure in 14.4.5 applies, and the procedure terminates. Any resultant new report is processed from the start of this procedure.

2) A report received back from the Report-out procedure has encountered a transfer failure in the process of relaying to another MTA. The Report-routing procedure attempts to re-route such a report, i.e., compute an alternative next hop address (subject to the security-policy in force). If an alternative next hop address is found then the report, together with this information and suitably modified trace information is returned as the procedure's result. The procedure then terminates. The report is subsequently passed to the Report-out procedure.

If an alternative next hop address cannot be determined, then the report is discarded and the procedure terminates without returning a result.

14.4.5 Double-enveloper Procedure

This procedure takes a report on a message (created by this MTA) which had an inner-envelope content-type, and if it is a non-delivery report then it substitutes a non-delivery report on the message that was in the inner-envelope.

14.4.5.1 Arguments

A report.

14.4.5.2 Results

Another report if the argument is a non-delivery report, or none otherwise.

14.4.5.3 Errors

None.

14.4.5.4 Procedure Description

If the report is a non-delivery report, then the record of submitted double-enveloped messages is read to obtain the information necessary to create a non-delivery report on the inner-envelope message. This new non-delivery report replaces the non-delivery report on the outer-envelope.

If the report is a delivery report, then no further transfer of it is required.

In either case, the record of submitted double-enveloped messages is augmented with information about the delivery or non-delivery report. The MTA may implement an additional procedure, activated by expiry of a timer, to generate a non-delivery report on the inner-envelope message if no delivery report has been received on the outer-envelope message.

14.5 MTS-bind and MTS-unbind

14.5.1 MTS-user initiated MTS-bind Procedure

This clause describes the behaviour of the MTA when an MTS-bind is invoked by an MTS-user.

14.5.1.1 Arguments

The MTS-bind arguments are defined in 8.1.1.1.1.

14.5.1.2 Results

The MTS-bind results are defined in 8.1.1.1.2.

14.5.1.3 Errors

The bind-errors are defined in 8.1.2.

14.5.1.4 Procedure Description

1) If the MTAs resources cannot currently support the establishment of a new association, the procedure returns a Busy bind-error and terminates.

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

2) Otherwise, if authentication is required by the security-policy, the MTA attempts to both authenticate the MTS-user via the **initiator-credentials** supplied and check the acceptability of the **security-context**.

   If the **initiator-credentials** contain **strong-credentials**, the signature of the initiator-bind-token is verified using the public key from the MTS-user's **certificate** for the identified signature algorithm. The MTS-user's **certificate** may be included in initiator-credentials in the Bind argument, or identified by a **certificate-selector** and, if not already available to the MTA, obtained from the MTS-user's User Certificate attribute in the Directory. The validity of the **certificate** and its certification-path are also verified. Additionally, the Directory name from the subject field of that Certificate is verified to be that of the MTS-user. The **OR-name** in the subject-alternative-name field of that Certificate is verified to correspond to the **OR-name** of the MTS-user, and to correspond to the **OR-name** present in the initiator-name field of Bind. The mta-name and global-domain-identifier within initiator-bind-token are verified as being those of this MTA. The Time in the token is compared with the current time to ensure that the validity period of the token acceptable to this MTA has not expired.

   The responder-bind-token is generated by using the same signature algorithm (unless a preferred alternative is known to be supported by the MTS-user) and this MTA's private key to sign a token which comprises the algorithm-identifier for the signature algorithm, the **OR-name** of the MTS-user, the current time, and a random number as the bind-token-signed-data. This responder-bind-token together with either the **certificate-selector** or the **certificate** (and the additional certificates which provide its certification-path) for this MTA's public key for this algorithm form the responder-credentials in the Bind result.

   If the **initiator-credentials** cannot be authenticated, the procedure returns an authentication-error and terminates. If the **security-context** is not acceptable, the procedure returns an unacceptable-security-context bind-error and terminates.

3) If authentication is successful and the **security-context** is acceptable then the MTA accepts the requested association. The procedure returns the **MTA-name** and **responder-credentials**. **Messages-waiting** is also returned if the MTS-user subscribes to the Hold for Delivery element-of-service. The procedure then terminates.

4) If authentication is not required, **messages-waiting** is returned if the MTS-user subscribes to the Hold for Delivery element-of-service, and the procedure terminates.

14.5.2 MTS-user initiated MTS-unbind Procedure

This clause describes the behaviour of the MTA when an MTS-unbind is invoked by an MTS-user in order to release an existing association established by the MTS-user.

14.5.2.1 Arguments

None.

14.5.2.2 Results

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

14.5.2.3 Errors

None.

14.5.2.4 Procedure Description

The procedure releases the association, returns an empty result, and terminates.

14.5.3 MTA initiated MTS-bind Procedure

This clause describes the steps taken by an MTA when tasked to establish an association with an MTS-user.

14.5.3.1 Arguments

The MTS-bind arguments are defined in 8.1.1.1.1.

14.5.3.2 Results

An internal identifier for the association established.

14.5.3.3 Errors

The procedure returns a failure indication in the event an association could not be established.

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

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

14.5.3.4 Procedure Description

1) The procedure establishes values for the arguments defined in 8.1.1.1.1. **Messages-waiting** may be supplied if the MTS-user subscribes to the Hold for Delivery element-of-service. Values for **initiator-name**, **security-context**, and **initiator-credentials** are taken from internal information.

   If the **initiator-credentials** is to contain **strong-credentials**, the MTA selects a signature algorithm which is supported by the MTS-user, and uses this algorithm to sign an initiator-bind-token comprising the algorithm-identifier for this algorithm, the **OR-name** of the MTS-user, the current time, and a random number as the bind-token-signed-data. This initiator-bind-token together with either the **certificate-selector** or the **certificate** (and the additional certificates which provide its certification-path) for this MTA's public key for this algorithm form the initiator-credentials in the Bind argument.

2) The procedure determines the **user-address** of the MTS-user and attempts to establish an association with the arguments of 8.1.1.1.1. If unsuccessful a failure indication is returned and the procedure terminates.

3) If successful, the results returned from the MTS-user (defined in 8.1.1.1.2) are examined. The **responder-name** is checked for correctness and an attempt is made to authenticate the MTS-user via the **responder-credentials** returned.

   When the Bind result is received, the signature of the responder-bind-token is verified using the public key from the MTS-user's **certificate** for the identified signature algorithm. (This might be a different signature algorithm to the one used to sign the initiator-bind-token.) The MTS-user's **certificate** may be included in the Bind result, or identified by a **certificate-selector** and, if not already available to the MTA, obtained from the MTS-user's User Certificate attribute in the Directory. The validity of the **certificate** and its certification-path are also verified. Additionally, the Directory name from the subject field of that **certificate** is verified to be that of the MTS-user (i.e. that the responding MTS-user is the intended target of the Bind). The **OR-name** in the subject-alternative-name field of that **certificate** is verified to correspond to the **OR-name** of the MTS-user, and to correspond to the **OR-name** present in the responder-name field of Bind result. The mta-name and global-domain-identifier within responder-bind-token are verified as being those of this MTA. The Time in the token is compared with the current time to ensure that the validity period of the token acceptable to this MTA has not expired.

   If either check fails, the procedure closes the connection, returns a failure indication, and terminates.

4) If both checks are successful the procedure returns the association identifier and terminates.

14.5.4 MTA initiated MTS-unbind Procedure

This procedure is called to release an association with an MTS-user.

14.5.4.1 Arguments

The internal identifier for the association to be released.

14.5.4.2 Results

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

14.5.4.3 Errors

None.

14.5.4.4 Procedure Description

The procedure releases the association, returns an empty result, and terminates.

14.6 Submission Port

14.6.1 Message-submission Procedure

This clause describes the behaviour of the MTA when the Message-submission abstract-operation is invoked by the MTS-user on a submission port.

14.6.1.1 Arguments

The Message-submission arguments listed in Table 3 and described in clauses indicated in that table.

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

14.6.1.2 Results

1) The Message-submission results listed in Table 5 and described in clauses indicated in that table are passed back to the MTS-user.

2) The Deferred Delivery module is invoked and passed the submitted message.

14.6.1.3 Errors

See 8.2.1.1.3 for descriptions of the relevant abstract-errors.

14.6.1.4 Procedure Description

1) Error Checking

   The Message-submission procedure checks for error conditions. If any is found, the indicated abstract-error is returned. All further processing is terminated. Responsibility for the intended message is not accepted by the MTA.

   Errors of particular interest:

   a) Security errors. If the **message-security-label** is not compatible with the **security-context** or, if required, the **message-origin-authentication-check** is incorrect, a security-error is generated.

   b) Criticality errors. If any of the extension fields is marked **critical-for-submission**, but not semantically understood by the MTA, an unsupported-critical-function-error is returned.

      If no errors are encountered at this stage, processing continues at step 2. Additional errors may be encountered in these later processing stages, in which case the MTA takes action as described above.

2) Name Processing

   The following procedure applies to **originator-name**, **recipient-name** and **originator-requested-alternate-recipient**, unless otherwise noted.

   a) If the **OR-name** contains only a **directory-name**, the MTA attempts to obtain the **OR-address**.

      In the case of **recipient-name**, the Directory Name Resolution procedure (see 14.3.12) is called to determine a new **OR-address**.

      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.

   b) If the **OR-name** contains both the **directory-name** and the **OR-address**, their association need not be validated.

   c) The validation of the **OR-address**, whether passed in the Message-submission argument or obtained by resolving the **directory-name**, has two steps. The first step validates that the purported **OR-address** has the combination of attributes needed for a valid **OR-address** (see 8.5.5). The second step, which applies only to the **originator-name**, validates that the **OR-address** is, in fact, an **OR-address** of the MTS-user submitting the message.

3) Transfer of Responsibility, Return of Results

   If no errors are detected in the above processing, the MTA accepts responsibility for the message and so signifies by returning the Message-submission results to the MTS-user. The Message-submission results are described in 8.2.1.1.2. The **message-submission-identifier** and **message-submission-time** arguments are constructed as appropriate by the MTA. The **content-identifier** is identical to the corresponding Message-submission argument. If requested by the originator, the originating-MTA generates the **proof-of-submission** using the algorithm identified by the **proof-of-submission-algorithm-identifier** and the arguments defined in 8.2.1.1.2.4. In addition the **originating-MTA-certificate** is returned.

4) Message Construction

   A Message is constructed from the Message-submission arguments, as possibly modified in the above processing steps, plus additional arguments supplied by the MTA, as specified in 12.2.1.1.

   When complete, the Message-submission procedure terminates and the message is passed to the Deferred Delivery module for further processing.

14.6.2 Probe-submission Procedure

This clause describes the behaviour of the MTA when the Probe-submission abstract-operation is invoked by the MTS-user on a submission-port.

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

14.6.2.1 Arguments

The Probe-submission arguments listed in Table 7 and described in clauses indicated in that table.

14.6.2.2 Results

1) The Probe-submission results listed in Table 8 and described in clauses indicated in that table are passed back to the MTS-user.

2) The Main module is invoked and passed the submitted probe.

14.6.2.3 Errors

See 8.2.1.2.3 for descriptions of the relevant abstract-errors.

14.6.2.4 Procedure Description

1) Error Checking

   The Probe-submission procedure checks for error conditions. If any is found, the indicated abstract-error is returned. Responsibility for the intended probe is not accepted by the MTA.

   Errors of particular interest:

   a) Security errors. If the **message-security-label** is not compatible with the security-context, or if the **probe-origin-authentication-check** is incorrect, a security-error is generated.

   b) Criticality errors. If any of the extension-fields is **critical-for-submission**, but not semantically understood by the MTA, an unsupported-critical-function-error is returned.

      If no errors are encountered at this stage, processing continues at step 2. Additional errors may be encountered in these later processing stages, in which case the MTA takes action as described above.

2) Name Processing

   The following procedure applies to **originator-name**, **recipient-name** and **originator-requested-alternate-recipient**, unless otherwise noted.

   a) If the **OR-name** contains only a **directory-name**, the MTA attempts to obtain the **OR-address**.

      In the case of **recipient-name**, the Directory Name Resolution procedure (see 14.3.12) is called to determine a new **OR-address**.

      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.

   b) If the **OR-name** contains both the **directory-name** and the **OR-address**, their association need not be validated.

   c) The validation of the **OR-address**, whether passed in the Probe-submission argument or obtained by resolving the **directory-name**, has two steps. The first step validates that the purported **OR-address** has the combination of attributes needed for a valid **OR-address** (see 8.5.5). The second step, which applies only to the **originator-name**, validates that the **OR-address** is, in fact, the **OR-address** of the MTS-user submitting the message.

3) Transfer of Responsibility, Return of Results

   If no errors are detected in the above steps, the MTA accepts responsibility for the probe and so signifies by returning the Probe-submission results to the MTS-user. The Probe-submission results are described in 8.2.1.2.2. The **probe-submission-identifier** and **probe-submission-time** arguments are constructed as appropriate by the MTA. The **content-identifier** is identical to the corresponding Probe-submission argument.

4) Probe Construction

   A probe is constructed from the Probe-submission arguments, as possibly modified in the above processing steps, plus additional arguments supplied by the MTA.

   When complete, the Probe-submission procedure terminates and the probe is passed to the Main module for further processing.

14.6.3 Cancel-deferred-delivery Procedure

This clause describes the behaviour of the MTA when the Cancel-deferred-delivery abstract-operation is invoked by the MTS-user on a submission-port in order to cancel the deferred delivery message previously submitted to the MTA.

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

14.6.3.1 Arguments

The Cancel-deferred-delivery arguments listed in Table 10 and described in clauses indicated in that table.

14.6.3.2 Results

An empty result is passed back to the MTS-user as an indication of successful cancellation.

14.6.3.3 Errors

See 8.2.1.3.3 for descriptions of the relevant abstract-errors.

14.6.3.4 Procedure Description

1) If a **proof-of-submission** has already been provided, the Too-late-to-cancel abstract-error is returned by the MTA. The deferred delivery of the message is not cancelled.
2) If the value of the **message-submission-identifier** argument is recognized by the MTA as being valid and associated with a message being held by the MTA for deferred-delivery, the MTA discards this message as being cancelled, and assumes no further responsibility for it.
3) If the value of the **message-submission-identifier** argument is recognized by the MTA as being valid but refers to a message already delivered or transferred to another MTA, the Too-late-to-cancel abstract-error is invoked by the MTA. The deferred delivery of the message is not cancelled.
4) If the value of the **message-submission-identifier** argument is not recognized as being valid (either because the MTA never assigned such a value or because the MTA no longer holds the historical record of a deferred delivery message that has been transferred or delivered), then the Message-submission-identifier-invalid or Too-late-to-cancel abstract-error is returned by the MTA, the choice of which being a local matter.

14.6.4 Submission-control Procedure

This clause describes the behaviour of the MTA when invoking the Submission-control abstract-operation on a submission-port in order to temporarily limit the submission-port abstract-operations that the MTS-user can invoke. These controls remain in force for the duration of the current association unless overridden by a subsequent Submission-control abstract-operation.

NOTE – The use of Submission-control shall be subject to the security-policy in force. The **permissible-security-context** Submission-control argument limits the **security-context** established during the MTS-bind.

14.6.4.1 Arguments

The Submission-control arguments listed in Table 12 and described in clauses indicated in that table.

14.6.4.2 Results

The Submission-control results listed in Table 13 and described in clauses indicated in that table are passed back to the MTA by the MTS-user.

14.6.4.3 Errors

A Security-error can be passed back by the MTS-user. See 8.2.1.4.3 for a description of this abstract-error.

14.6.4.4 Procedure Description.

The circumstances causing an MTA to invoke the Submission-control abstract-operation are a local matter, as are the actions taken during and subsequent to its completion.

14.7 Delivery Port

14.7.1 Message-delivery Procedure

This clause describes the steps taken by an MTA when tasked to deliver a message to one or more MTS-users.

Most provisions of this clause also apply to the case where the MTA has received a probe with one or more local recipients. Unless noted otherwise, all procedure steps save physical delivery apply to the handling of probes.

NOTE – The generation of reports shall be subject to the security-policy.

14.7.1.1 Arguments

1) A message from the Main module with per-recipient instructions to deliver to one or more local MTS-users.

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

2) The Message-delivery arguments listed in Table 15 and described in clauses indicated in that table are passed to the recipient MTS-user.

14.7.1.2 Results

1) An empty result or, if requested, a **proof-of-delivery** and optional **recipient-certificate** passed back from the MTS-user as an indication of successful delivery with no reporting requirements,
2) If a report is required, the Main module is invoked and passed the message with per-recipient instructions describing any delivery problems encountered and/or indicating successful deliveries to be reported on.

14.7.1.3 Errors

Message-delivery abstract-errors that can be returned from the MTS-user to the MTA are described in 8.3.1.1.3. These error conditions are reported to the Main module in the results described above.

14.7.1.4 Procedure Description

1) If the message expiration is reached, a report instruction is generated for each local recipient. The values of **non-delivery-reason-code** and **non-delivery-diagnostic-code** are **unable-to-transfer** and **maximum-time-expired**, respectively. The procedure then terminates.
2) If any of the per-message **extension-fields** is set to **critical-for-delivery** but not semantically understood by the MTA, a report instruction for each local recipient is generated. The values of **non-delivery-reason-code** and **non-delivery-diagnostic-code** are set to **unable-to-transfer** and **unsupported-critical-function** respectively.
3) Otherwise, values are established for those arguments to the Message-delivery abstract-operation that apply to all recipients (arguments to Message-delivery are described in 8.3.1.1.1).
4) Steps 5-16 are executed for each recipient with **responsibility** set to **responsible**. The procedure then terminates.
5) To ensure the security-policy is not violated during delivery, the **message-security-label** is checked against the **security-context**. If delivery is barred by the security-policy then, subject to the security-policy, a report instruction for this is generated. The values of **non-delivery-reason-code** and **non-delivery-diagnostic-code** are **unable-to-transfer** and **secure-messaging-error**, respectively.
6) If delivery is barred by Delivery Controls imposed in a previously invoked Register or Delivery-control abstract-operation, then, subject to the security-policy in force, the MTA will hold the message pending the lifting of the applicable controls. Delivery Controls are not applicable to probes.
7) If the maximum holding time for a held message (the value of this maximum time being a local matter, except that **latest-delivery-time** shall be observed when present and **critical-for-delivery**) expires with the applicable restrictions still in effect, then a report instruction is generated for this recipient. The values of **non-delivery-reason-code** and **non-delivery-diagnostic-code** are **unable-to-transfer** and **recipient-unavailable**, respectively. Processing then terminates for this recipient.

   NOTE – The processing steps (6 and 7 above) associated with control restrictions do not apply in the case of Probe.
8) If restricted-delivery is enforced, and the sender falls in the category of unauthorised senders, then a report instruction is generated for this recipient. The values of **non-delivery-reason-code** is set to **restricted-delivery**. Processing then terminates for this recipient.
9) The MTA establishes those arguments for the Message-delivery abstract-operation that apply only to the individual recipient: **message-delivery-identifier** and **message-delivery-time** are given values as described in Clauses 8.3.1.1.1.1 and 8.3.1.1.1.2. If the message contains a **redirection-history** or a **dl-expansion-history** then the **originally-intended-recipient-name** shall be copied from the first element of either the **redirection-history** or the **dl-expansion-history**, whichever event occurred first (and the sequence of these events shall be determined from the **trace-information**). All other arguments are taken directly from corresponding fields of the message to be delivered. With the exceptions noted below, all arguments shown in Table 15 are included in each invocation of Message-delivery.
10) If **disclosure-of-other-recipients** has the value **disclosure-of-other-recipients-requested**, the **other-recipient-name** argument is set to include the following:
    a) The **OR-names** of all originally-specified recipients with an **originally-specified-recipient-number** distinct from that for the current recipient. For any such recipient for which redirection has been recorded, the originally-specified recipient's **OR-name** is that from the first entry in the associated redirection-history;
    b) If distribution list expansion has occurred, the **OR-name** from the first entry of the **DL-expansion-history**.

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

If the recipient is a member of a distribution list, other members of this distribution list must not be included in the **other-recipient-name** argument. The recipient is a member of a distribution list if the **DL-expansion-history** field is non-empty.

11) If any of the per-recipient **extension-fields** is set to **critical-for-delivery**, but not semantically understood by the MTA, a report instruction for this recipient is generated. The values of the **non-delivery-reason-code** and **non-delivery-diagnostic-code** are set to **unable-to-transfer** and **unsupported-critical-function** respectively.

12) In the case of delivery to a Physical Delivery Access Unit, the Physical Delivery Arguments are included in the Message-delivery. These arguments are described in clauses 8.2.1.1.1.14 – 8.2.1.1.1.23.

13) Once all conditions have been met for successful delivery, the MTA will physically deliver the message. The accomplishment of delivery to a co-located recipient MTS-user is a local matter. In the case of a remotely located recipient MTS-user, the MTA establishes an association with that MTS-user (or uses an existing one) and invokes the Message-delivery abstract-operation across that association. With successful delivery, either remote or local, responsibility for the message passes from the MTA to the recipient MTS-user.

14) Upon a successful delivery, if the **originating-MTA-delivery-report-request** has the value of **report** or **audited-report**, then a report instruction is generated noting the successful delivery. Processing then terminates for this recipient.

15) In the case of a remotely located recipient MTS-user, if an association neither exists nor can be established initially, or there is a transfer failure across an association, the MTA can repeat the attempt at association establishment and/or transfer, the maximum number and/or time duration of repeats being a local matter (except that **latest-delivery-time** shall be observed when present and **critical-for-delivery**). If, after repeated attempts transfer has not been accomplished, the message is deemed undeliverable and, subject to the security-policy in force, a report instruction is generated. The values of **non-delivery-reason-code** and **non-delivery-diagnostic-code** are **transfer-failure** and **recipient-unavailable**, respectively. Processing then terminates for this recipient.

NOTE – The processing steps associated with physical transfer of a message to the recipient MTS-user do not apply in the case of Probe.

16) Return of Results and Errors by the MTS-user

If the Message-delivery abstract-operation is successful, then the MTS-user returns as an indication of success either an empty result or, if requested, a **proof-of-delivery** and optional **recipient-certificate**.

If the Message-delivery abstract-operation violates one or more controls imposed by a previous Delivery-control or Register abstract-operation, then the MTS-user returns a Delivery-control-violated error. If the **security-context** dictates that the MTS-user cannot support the requested abstract-operation because it would violate the security-policy, then the MTS-user returns a Security-error. In this event the Message-delivery invocation has failed and the MTA retains responsibility for the message with respect to this recipient. The message is held for subsequent retry or is passed to the Main module for report generation. Processing then terminates for this recipient.

14.7.2 Probe-delivery-test Procedure

This clause describes the steps taken by an MTA when tasked to test the deliverability of a Probe.

NOTE – The use of Reports shall be subject to the security-policy.

14.7.2.1 Arguments

1) A probe from the internal procedure with per-recipient instructions to Probe-delivery-test to one or more local MTS-users.

14.7.2.2 Results

The Main module is invoked and passed the probe with per-recipient instructions describing whether or not the hypothetical delivery would have occurred and if not why not.

14.7.2.3 Errors

None.

14.7.2.4 Procedure Description

The logic for Message-delivery is described in 14.7.1. All steps in that clause except those specifically noted as inapplicable to Probe are executed.

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

14.7.3 Report-delivery Procedure

This clause describes the steps taken by an MTA when tasked to deliver a report to an MTS-user. Report-delivery is called for when an MTA receives a report, from Report-in or upon generation within this MTA, whose **originator-name** field specifies an MTS-user served by this MTA.

14.7.3.1 Arguments

1) A report from the Report module with per-recipient instructions to deliver to a local recipient.
2) The Report-delivery arguments listed in Table 18 and described in clauses indicated in that table are passed to the recipient MTS-user.

14.7.3.2 Results

An empty result passed back from the MTS-user as an indication of successful delivery.

14.7.3.3 Errors

Report-delivery errors that can be returned from the MTS-user to the MTA are described in 8.3.1.2.3.

14.7.3.4 Procedure Description

1) To ensure the security-policy is not violated during Report-delivery the **message-security-label** is checked against the security-context. If Report-delivery is barred by the security-policy, then the report is discarded.
2) If report delivery is barred by restrictions imposed in a previously invoked Register or Delivery-control abstract-operation, then, subject to the security-policy in force, the MTA will hold the report pending the lifting of the applicable restriction(s). Restrictions are established by arguments of the Delivery-control or Register abstract-operation as described in 8.3.1.3.1.

   If the maximum holding time for a held report (the value of this maximum time being a local matter) expires with the applicable restrictions still in effect, then the report is discarded.
3) Arguments for the Report-delivery abstract-operation are taken from corresponding fields of the report.
4) If any of the per-message or per-recipient **extension-fields** are set to **critical-for-delivery**, but not semantically understood by the MTA, the report is discarded.
5) The accomplishment of Report-delivery to a co-located MTS-user is a local matter. In the case of a remotely located MTS-user, the MTA establishes an association with that MTS-user (or uses an existing one) and invokes the Report-delivery abstract-operation across that association. With successful Report-delivery, either remote or local, responsibility for the report passes from the MTA to the MTS-user.
6) In the case of a remotely located MTS-user, if an association cannot be established initially, the MTA can repeat the attempt, the maximum number and/or time duration of repeats being a local matter. If, after repeated attempts no association has been established, the report is deemed undeliverable and is discarded.
7) Return of Results and Errors by the MTS-user

   If the Report-delivery abstract-operation is successful, then the MTS-user returns an empty result as an indication of success.

   If the Report-delivery abstract-operation violates one or more controls imposed by a previous Delivery-control or Register abstract-operation, then the MTS-user returns a Delivery-control-violated error. In this event the Report-delivery invocation has failed and the MTA retains responsibility for the report.

14.7.4 Delivery-control Procedure

This clause describes the behaviour of the MTA when the Delivery-control abstract-operation is invoked by an MTS-user served by this MTA. Delivery-control imposes and lifts restrictions on the Message-delivery and Report-delivery abstract-operations. These controls remain in force for the duration of the current association unless overridden by a subsequent Delivery-control. Delivery-controls temporarily limit the **security-context** but cannot cause a violation of the security-policy.

These controls do not apply to the processing of probes by the MTA.

14.7.4.1 Arguments

The Delivery-control arguments listed in Table 20 and described in 8.3.1.3.1.

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

14.7.4.2 Results

1) The Delivery-control results listed in Table 21 and described in 8.3.1.3.2 are passed back to the MTS-user by the MTA.
2) Various control parameters of the MTS-user held by this MTA are replaced by values carried in the Delivery-control arguments.

14.7.4.3 Errors

See 8.3.1.3.3 for a description of the relevant abstract-errors.

14.7.4.4 Procedure Description.

1) If the value of the **restrict** argument is **remove**, then all controls established by any previous Delivery-control are removed; the abstract-operation is complete, and the Result is returned to the MTS-user.
2) If the value of the **restrict** argument is **update**, and no other arguments are present, the request is considered to be valid and the Result returned to the MTS-user.

   In such cases all currently in force control values remain unchanged.
3) If the value of the **restrict** argument is **update**, and other arguments are present, those arguments are checked for compatibility with long term conditions specified by the most recent invocation of the Register abstract-operation on the administration-port (see 14.4.1). If no incompatibility is detected, and the update is permitted within the security-policy, the indicated updates are carried out, the abstract-operation is complete, and the Result is returned to the MTS-user.
4) If any of the following incompatibilities is detected with long term conditions, a Control-violates-registration abstract-error is returned by the MTA:
   a) The **permissible-encoded-information-types** has a type not specified among those allowed long term.
   b) The **permissible-content-types** has a content not specified among those allowed long term.
   c) The **permissible-maximum-content-length** exceeds the length allowed long term.
   d) The **permissible-security-context** is violated.

   In any of these error cases, the Delivery-control is discarded and not carried out.

14.8 Administration Port

14.8.1 Register Procedure

This clause describes the behaviour of the MTA when the Register abstract-operation is invoked by an MTS-user served by this MTA.

14.8.1.1 Arguments

The Register arguments listed in Table 23 and described in clauses indicated in that table.

14.8.1.2 Results

1) If the **retrieve-registrations** argument is present, then the Register procedure returns the requested registered information in the result. A Register extension argument may also cause extension results to be returned. Otherwise an empty result is returned to the MTS-user as an indication of success.
2) Various parameters of the MTS-user held by this MTA are replaced by values carried in the Register arguments.

14.8.1.3 Errors

See 8.4.1.1.3 for a description of the relevant abstract-errors.

14.8.1.4 Procedure Description

1) The Register arguments are checked for correct specification. If any is incorrectly specified, the Register procedure returns a Register-rejected error and terminates. Subject to local policy or subscription, the MTA may impose additional restrictions on the registrations which may be performed by the MTS-user; if these restrictions are not met, an abstract-error is returned to the MTS-user and no further steps are processed.
2) If the Register arguments are correctly specified, the values of MTS-user parameters are replaced by those of the Register arguments. If (in the 1994 Application Context) the **recipient-assigned-**

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

redirections argument contains a single **restriction** in which all source-types are permitted and the source-name omitted, or if (in the 1988 Application Context) the **recipient-assigned-alternate-recipient** argument contains the **OR-name** of the MTS-user, no **recipient-assigned-redirection** is registered. If the **retrieve-registrations** argument is present, then the requested registered information is returned.

14.8.2 MTS-user initiated Change-credentials Procedure

This clause describes the behaviour of the MTA when a Change-credentials abstract-operation is invoked by the MTS-user.

NOTE – All changes of credentials shall be subject to the security-policy in force.

14.8.2.1 Arguments

The Change-credentials arguments listed in Table 25 and described in 8.4.1.2.1.

14.8.2.2 Results

1) The Change-credentials procedure returns an empty result to the MTS-user as an indication of success.
2) The MTS-user's credentials held by this MTA are changed in accordance with the **new-credentials** argument.

14.8.2.3 Errors

A New-credentials-unacceptable or Old-credentials-incorrectly-specified abstract-error, as described in 8.4.1.2.3 and listed in Table 26.

14.8.2.4 Procedure Description

NOTE – All changes of credentials shall be subject to the security-policy in force.

1) If the value of the **old-credentials** argument is not the same as the credentials held by the MTA for the MTS-user invoking the abstract-operation, an Old-credentials-incorrectly-specified error is returned to the MTS-user and the Change-credentials procedure terminates.
2) Otherwise, the **new-credentials** argument is checked for validity. If found invalid (a local matter dictated by the security-policy) a New-credentials-unacceptable error is returned to the MTS-user and the Change-credentials procedure terminates.
3) Otherwise, the MTS-user's credentials held by this MTA are changed to the value of the **new-credentials** argument, an empty result is returned to the MTS-user as an indication of success, and the Change-credentials procedure terminates.

14.8.3 MTA initiated Change-credentials Procedure

This clause describes the behaviour of an MTA when changing its credentials held by a locally supported MTS-user.

NOTE – All changes of credentials shall be subject to the security-policy in force.

14.8.3.1 Arguments

The Change-credentials arguments listed in Table 25 and described in 8.4.1.2.1.

14.8.3.2 Results

The MTS-user returns an empty result to the Change-credentials procedure as an indication of success.

14.8.3.3 Errors

The MTS-user can return a New-credentials-unacceptable or Old-credentials-incorrectly-specified error, as described in 8.4.1.2.3 and listed in Table 26.

14.8.3.4 Procedure Description

NOTE – All changes of credentials shall be subject to the security-policy in force.

1) The procedure invokes the Change-credentials abstract-operation to change the MTA's credentials held by a locally supported MTS-user. The conditions causing an MTA to change its credentials are a local matter.
2) If either the New-credentials-unacceptable or Old-credentials-incorrectly-specified error is received back from the MTS-user, then the MTA must assume its credentials have not been changed. Further action can be undertaken as a local matter, after which the procedure terminates.

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

3) If an empty result is received back from the MTS-user, the MTA may assume the procedure has been successful and its credentials changed. The procedure terminates.

14.9 MTA-bind and MTA-unbind

14.9.1 MTA-bind-in Procedure

This clause describes the behaviour of the MTA when an MTA-bind is invoked by another MTA.

14.9.1.1 Arguments

The MTA-bind arguments are defined in 12.1.1.1.1 and listed in Table 28.

14.9.1.2 Results

The MTA-bind results are defined in 12.1.1.1.2 and listed in Table 29.

14.9.1.3 Errors

The bind-errors are defined in 12.1.2.

14.9.1.4 Procedure Description

1) If the MTA's resources cannot currently support the establishment of a new association, the procedure returns a Busy bind-error and terminates.

2) Otherwise, if authentication is required by the security-policy, the MTA attempts to both authenticate the calling MTA via the **initiator-credentials** supplied and check the acceptability of the security-context.

   If the **initiator-credentials** contain **strong-credentials**, the signature of the initiator-bind-token is verified using the public key from the initiating MTA's **certificate** for the identified signature algorithm. The initiating MTA's **certificate** may be included in initiator-credentials in the Bind argument, or identified by a **certificate-selector** and, if not already available to the MTA, obtained from the initiating MTA's User Certificate attribute in the Directory. The validity of the **certificate** and its certification-path are also verified. Additionally, the Directory name from the subject field of that Certificate is verified to be that of the initiating MTA. The mta-name in the subject-alternative-name field of that Certificate is verified to correspond to the calling MTA's MTA Name and Global Domain Identifier, and to correspond to the mta-name present in the initiator-name field of Bind. The mta-name and global-domain-identifier within initiator-bind-token are verified as being those of this MTA. The Time in the token is compared with the current time to ensure that the validity period of the token acceptable to this MTA has not expired.

   The responder-bind-token is generated by using the same signature algorithm (unless a preferred alternative is known to be supported by the initiator) and this MTA's private key to sign a token which comprises the algorithm-identifier for the signature algorithm, the mta-name and global domain identifier of the initiating MTA, the current time, and a random number as the bind-token-signed-data. This responder-bind-token together with either the **certificate-selector** or the **certificate** (and the additional certificates which provide its certification-path) for this MTA's public key for this algorithm form the responder-credentials in the Bind result.

   If the **initiator-credentials** cannot be authenticated, the procedure returns an authentication-error and terminates. If the **security-context** is not acceptable, the procedure returns an unacceptable-security-context error and terminates.

3) If authentication is successful and the **security-context** is acceptable, then the MTA establishes the requested association. The procedure returns the **MTA-name** and **responder-credentials**. The procedure then terminates.

4) If authentication is not required, there are no results to return and the procedure terminates.

14.9.2 MTA-unbind-in Procedure

This clause describes the behaviour of the MTA when an MTA-unbind is invoked by another MTA in order to release an existing association.

14.9.2.1 Arguments

None.

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

14.9.2.2 Results

The MTA-unbind-in procedure returns an empty result as an indication of release of the association.

14.9.2.3 Errors

None.

14.9.2.4 Procedure Description

The procedure releases the association, returns an empty result, and terminates.

14.9.3 MTA-bind-out Procedure

This clause describes the steps taken by an MTA when tasked to establish an association with another MTA.

14.9.3.1 Arguments

1) The **MTA-name** of the MTA with which the association is to be established.
2) The **security-context** for the association.

14.9.3.2 Results

An internal identifier for the association established.

14.9.3.3 Errors

The procedure returns a failure indication in the event an association could not be established.

14.9.3.4 Procedure Description

1) The procedure establishes values for the arguments defined in 12.1.1.1.1. Values for **initiator-name**, **security-context**, and **initiator-credentials** are taken from internal information.

   If the **initiator-credentials** is to contain **strong-credentials**, the MTA selects a signature algorithm which is supported by the target MTA, and uses this algorithm to sign an initiator-bind-token comprising the algorithm-identifier for this algorithm, the mta-name and global domain identifier of the target MTA, the current time, and a random number as the bind-token-signed-data. This initiator-bind-token together with either the **certificate-selector** or the **certificate** (and the additional certificates which provide its certification-path) for this MTA's public key for this algorithm form the initiator-credentials in the Bind argument.

2) The procedure determines the address of the MTA and attempts to establish an association with the arguments of 12.1.1.1.1. If unsuccessful a failure indication is returned and the procedure terminates.

3) If successful, the results returned from the called MTA (defined in 12.1.1.1.2) are examined. The **responder-name** is checked for correctness, an attempt is made to authenticate the MTA via the **responder-credentials** returned.

   When the Bind result is received, the signature of the responder-bind-token is verified using the public key from the responding MTA's **certificate** for the identified signature algorithm. (This might be a different signature algorithm to the one used to sign the initiator-bind-token.) The responding MTA's **certificate** may be included in the Bind result, or identified by a **certificate-selector** and, if not already available to the MTA, obtained from the responding MTA's User Certificate attribute in the Directory. The validity of the **certificate** and its certification-path are also verified. Additionally, the Directory name from the subject field of that **certificate** is verified to be that of the target MTA (i.e. that the responding MTA is the intended target of the Bind). The mta-name in the subject-alternative-name field of that **certificate** is verified to correspond to the target MTA's MTA Name and Global Domain Identifier, and to correspond to the mta-name present in the responder-name field of Bind result. The mta-name and global-domain-identifier within responder-bind-token are verified as being those of this MTA. The Time in the token is compared with the current time to ensure that the validity period of the token acceptable to this MTA has not expired.

   If any of the checks fail, the procedure returns a failure indication to the caller, terminates the association, and terminates.

4) If all checks are successful the procedure returns the association identifier and terminates.

14.9.4 MTA-unbind-out Procedure

This procedure is called to release an association with another MTA.

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

14.9.4.1 Arguments

The internal identifier for the association to be released.

14.9.4.2 Results

The MTA-unbind-out procedure returns an empty result as an indication of release of the association.

14.9.4.3 Errors

None.

14.9.4.4 Procedure Description

The procedure releases the association, returns an empty result, and terminates.

14.10 Transfer Port

NOTE – The actions taken on the transfer-port are subject to the security-policy in force.

14.10.1 Message-in Procedure

This clause describes the behaviour of the MTA when a Message-transfer abstract-operation is invoked by another MTA on a transfer-port.

14.10.1.1 Arguments

The Message-transfer arguments listed in Table 30 and described in clauses indicated in that table.

14.10.1.2 Results

The Deferred-delivery module is invoked and passed the message transferred in.

14.10.1.3 Errors

None.

14.10.1.4 Procedure Description

On receipt of a message through the occurrence of a Message-transfer abstract-operation (invoked from a neighbour MTA), the Message-in procedure is invoked. This procedure simply passes the message to the Deferred-delivery module to determine the actions to be taken by this MTA.

Responsibility for the message passes to the receiving-MTA with the successful transfer.

14.10.2 Probe-in Procedure

This clause describes the behaviour of the MTA when a Probe-transfer abstract-operation is invoked by another MTA on a transfer-port.

14.10.2.1 Arguments

The Probe-transfer arguments listed in Table 31 and described in clauses indicated in that table.

14.10.2.2 Results

The Main module is invoked and passed the probe transferred in.

14.10.2.3 Errors

None.

14.10.2.4 Procedure Description

On receipt of a probe through the occurrence of a Probe-transfer abstract-operation (invoked from a neighbour MTA), the Probe-in procedure is invoked. This procedure simply passes the probe to the Main module to determine the actions to be taken by this MTA.

Responsibility for the probe passes to the receiving MTA with the successful transfer.

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

14.10.3 Report-in Procedure

This clause describes the behaviour of the MTA when it receives a Report on a transfer-port through the occurrence of a Report-transfer abstract-operation invoked by another MTA, or when it receives an indication for the generation of a report from an access unit such as a PDAU.

14.10.3.1 Arguments

The Report arguments listed in Table 32 and described in clauses indicated in that table.

14.10.3.2 Results

The Report module is invoked and passed the report transferred in.

14.10.3.3 Errors

None.

14.10.3.4 Procedure Description

On receipt of a report through the occurrence of a Report-transfer abstract-operation (invoked from a neighbour MTA), or on receipt of an indication for a report generation from an access unit such as a PDAU, the Report-in procedure is invoked. This procedure simply passes the report to the Report module to determine the actions to be taken by this MTA.

Responsibility for the report passes to the receiving-MTA with the successful transfer.

14.10.4 Message-out Procedure

This clause describes the steps taken by an MTA when tasked to transfer a message to another MTA.

14.10.4.1 Arguments

A message from the internal procedure with routing instructions to transfer to another MTA. The fields of this message form the arguments of the Message-transfer abstract-operation as listed in Table 30.

14.10.4.2 Results

None.

14.10.4.3 Errors

In case of transfer failure the Main module is invoked and passed the message with a per-message instruction indicating the failure reason.

14.10.4.4 Procedure Description

The message to be transferred provides the arguments for the Message-transfer abstract-operation. It should be noted that the message may reflect processing (e.g. content conversion, redirection, distribution list expansion) carried out in this or previous MTAs.

1) To ensure the security-policy is not violated during transfer, the **message-security-label** is checked against the **security-context**. If the transfer is barred by either the security-policy or temporary restrictions, then processing continues at step 3, below.

2) Otherwise, the MTA establishes an association with the receiving-MTA (or uses an existing one) and invokes the Message-transfer abstract-operation across that association. The completion of Message-out indicates that the transfer has been successful and that the receiving-MTA now accepts responsibility for the message. The Message-out procedure now terminates.

   If the sending-MTA has been instructed by the receiving system to abort the transfer, then the processing continues at step 3, below.

   If an association neither exists nor can be established initially, or there is a transfer failure across an association, the MTA can repeat the attempt at association establishment and/or transfer, the maximum number and/or time duration of repeats being a local matter, except that **latest-delivery-time** shall be observed when present and **critical-for-transfer**.

3) If, after repeated attempts transfer has not been accomplished, or a security violation has been detected in step 1, or the sending-MTA has been instructed to abort the transfer in step 2, the message is deemed non transferable and is returned, with failure reason indicated, to the Main module for possible re-routing or

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

redirection. Responsibility for the message remains with the sending MTA. The Message-out procedure now terminates.

NOTE – The instruction to abort a transfer is generated by the receiving RTSE-provider if it is permanently unable to complete the transfer; for example, when the transfer is of such a size that it could never be accepted.

14.10.5 Probe-out Procedure

This clause describes the steps taken by an MTA when tasked to transfer a probe to another MTA.

14.10.5.1 Arguments

A probe from the internal procedure with routing instructions to transfer to another MTA. The fields of this probe form the arguments of the Probe-transfer abstract-operation as listed in Table 31.

14.10.5.2 Results

None.

14.10.5.3 Errors

In case of transfer failure the Main module is invoked and passed the probe with a per-message instruction indicating the failure reason.

14.10.5.4 Procedure Description

The probe to be transferred provides the arguments for the Probe-transfer abstract-operation. It should be noted that the probe may reflect processing (e.g. redirection) carried out in this or previous MTAs.

1) To ensure the security-policy is not violated during transfer, the **message-security-label** is checked against the **security-context**. If the transfer is barred by either the security-policy or temporary restrictions, then processing continues at step 3, below.

2) The MTA establishes an association with the receiving MTA (or uses an existing one) and invokes the Probe-transfer abstract-operation across that association. The completion of Probe-out indicates that the transfer has been successful and that the receiving-MTA now accepts responsibility for the probe. The Probe-out procedure now terminates.

   If the sending-MTA has been instructed by the receiving system to abort the transfer, then the processing continues at step 3, below.

   If an association neither exists nor can be established initially, or there is a transfer failure across an association, the MTA can repeat the attempt at association establishment and/or transfer, the maximum number and/or time duration of repeats being a local matter.

3) If, after repeated attempts transfer has not been accomplished, or a security violation has been detected in step 1 above, or the sending-MTA has been instructed to abort the transfer in step 2, then the probe is deemed non transferable and is returned, with failure reason indicated, to the Main module for possible re-routing or redirection. Responsibility for the probe remains with the sending MTA. The Probe-out procedure now terminates.

NOTE – The instruction to abort a transfer is generated by the receiving RTSE-provider if it is permanently unable to complete the transfer; for example, when the transfer is of such a size that it could never be accepted.

14.10.6 Report-out Procedure

This clause describes the steps taken by an MTA when tasked to transfer a report to another MTA.

14.10.6.1 Arguments

A report from the internal procedure with routing instructions to transfer to another MTA. The fields of this report form the arguments of the Report-transfer abstract-operation as listed in Table 32.

14.10.6.2 Results

None.

14.10.6.3 Errors

The report, together with the reason for transfer failure, to be passed back to the Report module.

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

14.10.6.4 Procedure Description

The report to be transferred provides the arguments for the Report-transfer abstract-operation. It should be noted that the report may reflect processing (e.g. redirection) carried out in this or previous MTAs.

1) To ensure the security-policy is not violated during transfer, the **message-security-label** is checked against the **security-context**. If the transfer is barred by either the security-policy or temporary restrictions, then processing continues at step 3, below.

2) The MTA establishes an association with the receiving MTA (or uses an existing one) and invokes the Report-transfer abstract-operation across that association. The completion of Report-out indicates that the transfer has been successful and that the receiving-MTA now accepts responsibility for the report. The Report-out procedure now terminates.

   If the sending-MTA has been instructed by the receiving system to abort the transfer, then the processing continues at step 3, below.

   If an association neither exists nor can be established initially, or there is a transfer failure across an association, the MTA can repeat the attempt at association establishment and/or transfer, the maximum number and/or time duration of repeats being a local matter.

3) If, after repeated attempts transfer has not been accomplished, or a security violation has been detected in step 1 above, or the sending-MTA has been instructed to abort the transfer in step 2, then the report is deemed non transferable and is returned, with failure reason indicated, to the Report module for possible re-routing. Responsibility for the report remains with the sending MTA. The Report-out procedure now terminates.

NOTE – The instruction to abort a transfer is generated by the receiving RTSE-provider if it is permanently unable to complete the transfer; for example, when the transfer is of such a size that it could never be accepted.

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

Annex A

Reference Definition of MTS Object Identifiers

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

This annex defines for reference purposes various object identifiers cited in the ASN.1 modules in the body of this Service Definition. The object identifiers are assigned in Figure A.1.

All object identifiers this Service Definition assigns are assigned in this annex. The annex is definitive for all but those ASN.1 modules and the Message Transfer System itself. The definitive assignments for the former occur in the modules themselves; other references to them appear in IMPORT clauses. The latter is fixed.

```
MTSObjectIdentifiers { joint-iso-itu-t mhs(6) mts(3) modules(0) object-identifiers(0)
              version-1999(1) }
DEFINITIONS IMPLICIT TAGS ::=
BEGIN

--      Prologue

--      Exports everything

IMPORTS-- nothing --  ;

ID ::= OBJECT IDENTIFIER

--      Message Transfer System

id-mts ID ::= { joint-iso-itu-t mhs(6) mts(3) } -- not definitive

--      Categories of Object Identifiers

id-mod  ID ::= { id-mts 0 } -- modules
id-ot   ID ::= { id-mts 1 } -- object types
id-pt   ID ::= { id-mts 2 } -- port types
id-cont ID ::= { id-mts 3 } -- content types
id-eit  ID ::= { id-mts 4 } -- encoded information types
id-att  ID ::= { id-mts 5 } -- attributes
id-tok  ID ::= { id-mts 6 } -- token types
id-sa   ID ::= { id-mts 7 } -- secure agent types
id-ct   ID ::= { id-mts 8 } -- contracts
id-cp   ID ::= { id-mts 9 } -- connection packages

--      Modules

id-mod-object-identifiers   ID ::= { id-mod 0 } -- not definitive
id-mod-mts-abstract-service ID ::= { id-mod 1 } -- not definitive
id-mod-mta-abstract-service ID ::= { id-mod 2 } -- not definitive
id-mod-upper-bounds         ID ::= { id-mod 3 } -- not definitive

--      Object Types

id-ot-mts      ID ::= { id-ot 0 }
id-ot-mts-user ID ::= { id-ot 1 }
id-ot-mta      ID ::= { id-ot 2 }
```

Figure A.1 – Abstract Syntax Definition of the MTS Object Identifiers (Part 1 of 2)

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

```
--      Port Types

id-pt-submission     ID  ::= { id-pt 0 }
id-pt-delivery       ID  ::= { id-pt 1 }
id-pt-administration ID  ::= { id-pt 2 }
id-pt-transfer       ID  ::= { id-pt 3 }

--      Content Types

id-cont-unidentified   ID ::= { id-cont 0 } -- For use by MS and Directory
id-cont-inner-envelope ID ::= { id-cont 1 }


--      Encoded Information Types

id-eit-unknown      ID ::= { id-eit 0 }
        -- Value { id-eit 1 } is no longer defined
id-eit-ia5-text     ID ::= { id-eit 2 }
id-eit-g3-facsimile ID ::= { id-eit 3 }
id-eit-g4-class-1   ID ::= { id-eit 4 }
id-eit-teletex      ID ::= { id-eit 5 }
id-eit-videotex     ID ::= { id-eit 6 }
id-eit-voice        ID ::= { id-eit 7 }
id-eit-sfd          ID ::= { id-eit 8 }
id-eit-mixed-mode   ID ::= { id-eit 9 }

--      Attributes

id-att-physicalRendition-basic         ID ::= { id-att 0 }
id-att-physicalRendition-no-cover-page ID ::= { id-att 1 }

--      Token Types

id-tok-asymmetricToken ID ::= { id-tok 0 }

--      Secure Agent Types

id-sa-ua ID ::= { id-sa 0 }
id-sa-ms ID ::= { id-sa 1 }

--      Contracts

id-ct-mts-access        ID ::= {id-ct 0}
id-ct-mts-forced-access ID ::= {id-ct 1}
id-ct-mta-transfer      ID ::= {id-ct 2}

--      Connection Packages

id-cp-mts-connect       ID ::= {id-cp 0}
id-cp-mta-connect       ID ::= {id-cp 1}

END     -- of MTSObjectIdentifiers
```

Figure A.1 – Abstract Syntax Definition of the MTS Object Identifiers (Part 2 of 2)

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

Annex B

Reference Definition of MTS Parameter Upper Bounds

(This Annex forms an integral part of the ITU-T Recommendation but does not form an integral part of the ISO/IEC International Standard)

This annex presents for reference purposes the upper bounds of various variable length data types whose abstract syntaxes are defined in the ASN.1 modules in the body of this Service Definition. The upper bounds are defined in Figure B.1.

```
MTSUpperBounds { joint-iso-itu-t mhs(6) mts(3) modules(0) upper-bounds(3) version-1999(1) }

DEFINITIONS IMPLICIT TAGS ::=

BEGIN

-- Prologue

-- Exports everything

IMPORTS-- nothing -- ;

-- Upper Bounds

ub-additional-info INTEGER ::= 1024

ub-bilateral-info INTEGER ::= 1024

ub-bit-options INTEGER ::= 16

ub-built-in-content-type INTEGER ::= 32767

ub-built-in-encoded-information-types INTEGER ::= 32

ub-certificates INTEGER ::= 64

ub-common-name-length INTEGER ::= 64

ub-content-correlator-length INTEGER ::= 512

ub-content-id-length INTEGER ::= 16

ub-content-length INTEGER ::= 2147483647          -- the largest integer in 32 bits

ub-content-types INTEGER ::= 1024

ub-country-name-alpha-length INTEGER ::= 2

ub-country-name-numeric-length INTEGER ::= 3

ub-diagnostic-codes INTEGER ::= 32767

ub-deliverable-class INTEGER ::= 256

ub-dl-expansions INTEGER ::= 512

ub-domain-defined-attributes INTEGER ::= 4
```

Figure B.1 – Abstract Syntax Definition of MTS Upper Bounds (Part 1 of 3)

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

```
ub-domain-defined-attribute-type-length INTEGER ::= 8

ub-domain-defined-attribute-value-length INTEGER ::= 128

ub-domain-name-length INTEGER ::= 16

ub-encoded-information-types INTEGER ::= 1024

ub-extension-attributes INTEGER ::= 256

ub-extension-types INTEGER ::= 256

ub-e163-4-number-length INTEGER ::= 15

ub-e163-4-sub-address-length INTEGER ::= 40

ub-generation-qualifier-length INTEGER ::= 3

ub-given-name-length INTEGER ::= 16

ub-initials-length INTEGER ::= 5

ub-integer-options INTEGER ::= 256

ub-labels-and-redirections INTEGER ::= 256

ub-local-id-length INTEGER ::= 32

ub-mta-name-length INTEGER ::= 32

ub-mts-user-types INTEGER ::= 256

ub-numeric-user-id-length INTEGER ::= 32

ub-organization-name-length INTEGER ::= 64

ub-organizational-unit-name-length INTEGER ::= 32

ub-organizational-units INTEGER ::= 4

ub-orig-and-dl-expansions INTEGER ::= 513   -- ub-dl-expansions plus one

ub-password-length INTEGER ::= 62

ub-pds-name-length INTEGER ::= 16

ub-pds-parameter-length INTEGER ::= 30

ub-pds-physical-address-lines INTEGER ::= 6

ub-postal-code-length INTEGER ::= 16

ub-privacy-mark-length INTEGER ::= 128

ub-queue-size INTEGER ::= 2147483647                    -- the largest integer in 32 bits

ub-reason-codes INTEGER ::= 32767

ub-recipient-number-for-advice-length INTEGER ::= 32

ub-recipients INTEGER ::= 32767

ub-redirection-classes INTEGER ::= 256

ub-redirections INTEGER ::= 512
```

Figure B.1 – Abstract Syntax Definition of MTS Upper Bounds (Part 2 of 3)

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

```
ub-restrictions INTEGER ::= 1024

ub-security-categories INTEGER ::= 64

ub-security-labels INTEGER ::= 256

ub-security-problems INTEGER ::= 256

ub-supplementary-info-length INTEGER ::= 256

ub-surname-length INTEGER ::= 40

ub-teletex-private-use-length INTEGER ::= 128

ub-terminal-id-length INTEGER ::= 24

ub-transfers INTEGER ::= 512

ub-tsap-id-length INTEGER ::= 16

ub-unformatted-address-length INTEGER ::= 180

ub-universal-generation-qualifier-length INTEGER ::= 16

ub-universal-given-name-length INTEGER ::= 40

ub-universal-initials-length INTEGER ::= 16

ub-universal-surname-length INTEGER ::= 64

ub-x121-address-length INTEGER ::= 16


END     -- of MTSUpperBounds
```

Figure B.1 – Abstract Syntax Definition of MTS Upper Bounds (Part 3 of 3)

NOTE – As specified in 45.5.4 of ITU-T Rec. X.680 | ISO/IEC 8824-1, upper bounds on TeletexString are measured in characters. A significantly greater number of octets will be required to hold such a value. As a minimum, 16 octets, or twice the specified upper bound, whichever is the larger, should be allowed.

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

Annex C

Definition of 1988 Message Transfer System Abstract Service

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

This annex defines a version of the Message Transfer System Abstract Service which, when realised in protocol, will interwork with the corresponding protocol defined in the previous edition of this Standard. It is provided for transition purposes only. This Annex is expected to be removed from the next edition.

The 1988 Message Transfer System Abstract Service is identical to the 1994 version defined in clause 8 except for the Register and Delivery-control operations which are defined below, and in the following cases: in the MTSBindArgument, MTSBindResult, InitiatorCredentials, ResponderCredentials, MessageDeliveryResult, and ReportDeliveryResult defined in Figure 2, components which follow the ellipsis ("...") are not defined for 1988 Application Contexts.

C.1 Register-88

The Register-88 abstract-operation enables an MTS-user to make long-term changes to various parameters of the MTS-user held by the MTS concerned with delivery of messages to the MTS-user.

Such changes remain in effect until overridden by re-invocation of the Register-88 abstract-operation. However, some parameters may be temporarily overridden by invocation of the Delivery-control-88 abstract-operation.

NOTE 1 – This abstract-operation shall be invoked before any other submission-port, delivery-port or administration-port abstract-operation may be used, or an equivalent registration by local means shall have taken place.

NOTE 2 – This abstract-operation does not encompass the standing parameters implied by the Alternate Recipient Assignment element-of-service and the Restricted Delivery element-of-service defined in ITU-T Rec. X.400 | ISO/IEC 10021-1. The manner in which those parameters are supplied and modified are a local matter.

C.1.1 Arguments

Table C.1 lists the arguments of the Register-88 abstract-operation, and for each argument qualifies its presence and identifies the clause in which the argument is defined.

Table C.1 – Register-88 Arguments

Argument	Presence	Clause
Registration Arguments		
User-name	O	8.4.1.1.1.1
User-address	O	8.4.1.1.1.2
Deliverable-encoded-information-types	O	C.1.1.1
Deliverable-content-types	O	C.1.1.2
Deliverable-maximum-content-length	O	C.1.1.3
Recipient-assigned-alternate-recipient	O	C.1.1.4
User-security-labels	O	C.1.1.5
Default Delivery Control Arguments		8.4.1.1.1.7
Restrict	O	8.3.1.3.1.1
Permissible-operations	O	8.3.1.3.1.2
Permissible-lowest-priority	O	8.3.1.3.1.3
Permissible-encoded-information-types	O	C.2.1.1
Permissible-content-types	O	8.3.1.3.1.5
Permissible-maximum-content-length	O	8.3.1.3.1.6

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

C.1.1.1 Deliverable-encoded-information-types

This argument indicates the **encoded-information-types** that the MTS shall permit to appear in messages delivered to the MTS-user, if they are to be changed. It may be generated by the MTS-user.

The MTS shall reject as undeliverable any message for an MTS-user for which the MTS-user is not registered to accept delivery of all of the **encoded-information-types** of the message. The MTS-user may register to receive the **unknown encoded-information-type**. **Deliverable-encoded-information-types** also indicate the possible **encoded-information-types** which implicit conversion may usefully produce.

In the absence of this argument, the **deliverable-encoded-information-types** shall remain unchanged.

C.1.1.2 Deliverable-content-types

This argument indicates the **content-types** that the MTS shall permit to appear in messages delivered to the MTS-user, if they are to be changed. It may be generated by the MTS-user.

The MTS shall reject as undeliverable any message for an MTS-user for which the MTS-user is not registered to accept delivery of the **content-types** of the message. The MTS-user may register to receive the **unidentified content-type**.

In the absence of this argument, the **deliverable-content-types** shall remain unchanged.

C.1.1.3 Deliverable-maximum-content-length

This argument contains the **content-length**, in octets, of the longest-content message that the MTS shall permit to appear in messages delivered to the MTS-user, if it is to be changed. It may be generated by the MTS-user.

The MTS shall reject as undeliverable any message for an MTS-user for which the MTS-user is not registered to accept delivery of messages of its size.

In the absence of this argument, the **deliverable-maximum-content-length** of messages shall remain unchanged.

C.1.1.4 Recipient-assigned-alternate-recipient

This argument contains the **OR-name** of an alternate-recipient, specified by the MTS-user, to which messages are to be redirected, if the alternate-recipient is to be changed. It may be generated by the MTS-user. A different value of this argument may be specified for each value of **user-security-labels**.

If a **recipient-assigned-alternate-recipient** is registered and associated with a value of **user-security-labels**, messages bearing a matching **message-security-label** shall be redirected to the alternate-recipient. Messages bearing a **message-security-label** for which no **recipient-assigned-alternate-recipient** has been registered, shall not be redirected to a **recipient-assigned-alternate-recipient**.

If a single **recipient-assigned-alternate-recipient** is registered, and not associated with a value of **user-security-labels**, all messages shall be redirected to the alternate-recipient.

The **recipient-assigned-alternate-recipient** shall contain the **OR-name** of the alternate-recipient. If the **recipient-assigned-alternate-recipient** contains the **OR-name** of the MTS-user (see 8.4.1.1.1.1), no **recipient-assigned-alternate-recipient** is registered.

In the absence of this argument, the **recipient-assigned-alternate-recipient**, if any, remains unchanged.

C.1.1.5 User-security-labels

This argument contains the **security-labels** of the MTS-user, if they are to be changed. It may be generated by the MTS-user.

A **recipient-assigned-alternate-recipient** may be registered for any value of **user-security-labels**.

In the absence of this argument, the **user-security-labels** remain unchanged.

Some security-policies may only permit the **user-security-labels** to be changed in this way if a secure link is employed. Other local means of changing the **user-security-labels** in a secure manner may be provided.

C.1.2 Results

The Register-88 abstract-operation returns an empty result as indication of success.

C.1.3 Abstract-errors

Table C.2 lists the abstract-errors that may disrupt the Register-88 abstract-operation, and for each abstract-error identifies the clause in which the abstract-error is defined.

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

Table C.2 – Register-88 Abstract-errors

Abstract-error	Clause
Register-rejected	8.4.2.1
Remote-bind-error	8.2.2.10

C.2 Delivery-control-88

The Delivery-control-88 abstract-operation enables the MTS-user to temporarily limit the delivery-port abstract-operations that the MTS may invoke, and the messages that the MTS may deliver to the MTS-user via the Message-delivery abstract-operation.

The MTS shall 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, the MTS-user re-invokes the Delivery-control-88 abstract-operation, or the MTS-user invokes the administration-port Register-88 abstract-operation to impose constraints more severe than the specified controls.

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

C.2.1 Arguments

Table C.3 lists the arguments of the Delivery-control-88 abstract-operation, and for each argument qualifies its presence and identifies the clause in which the argument is defined.

Table C.3 – Delivery-control-88 Arguments

Argument	Presence	Clause
Delivery Control Arguments		
Restrict	O	8.3.1.3.1.1
Permissible-operations	O	8.3.1.3.1.2
Permissible-lowest-priority	O	8.3.1.3.1.3
Permissible-encoded-information-types	O	C.2.1.1
Permissible-content-types	O	8.3.1.3.1.5
Permissible-maximum-content-length	O	8.3.1.3.1.6
Permissible-security-context	O	8.3.1.3.1.7

C.2.1.1 Permissible-encoded-information-types

This argument indicates the only **encoded-information-types** that shall appear in messages that the MTS shall deliver to the MTS-user via the Message-delivery abstract-operation. It may be generated by the MTS-user.

The **permissible-encoded-information-types** specified shall be among those allowed long-term due to a previous invocation of the administration-port Register abstract-operation (**deliverable-encoded-information-types**).

In the absence of this argument, the **permissible-encoded-information-types** that the MTS may deliver to the MTS-user are unchanged. If there has been no previous invocation of the Delivery-control abstract-operation on the association, the default control registered with the MTS by means of the administration-port Register abstract-operation shall apply.

C.2.2 Results

The results of the Delivery-control-88 abstract-operation are identical to the results of the Delivery-control abstract-operation which are defined in 8.3.1.3.2.

C.2.3 Abstract-errors

Table C.4 lists the abstract-errors that may disrupt the Delivery-control-88 abstract-operation, and for each abstract-error identifies the clause in which the abstract-error is defined.

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

Table C.4 – Delivery-control-88 Abstract-errors

Abstract-error	Clause
Control-violates-registration	8.3.2.2
Security-error	8.3.2.3

```
MTSAbstractService88 { joint-iso-itu-t mhs(6) mts(3) modules(0) mts-abstract-service(1)
              version-1988(1988) }

DEFINITIONS IMPLICIT TAGS ::=

BEGIN


--      Prologue

--      Exports everything

IMPORTS

        -- Remote Operations

        CONTRACT
                ----
                FROM Remote-Operations-Information-Objects { joint-iso-itu-t
                        remote-operations(4) informationObjects(5) version1(0) }

        -- MTS Abstract Service Parameters

        ABSTRACT-OPERATION, change-credentials, ContentLength, ContentTypes, Controls,
        control-violates-registration, DefaultDeliveryControls, EncodedInformationTypes,
        message-delivery, MHS-OBJECT, mts-connect, operationObject1, PORT,
        RecipientAssignedAlternateRecipient, register-rejected, report-delivery, SecurityLabel,
        security-error, submission, UserAddress, UserName, Waiting
                ----
                FROM MTSAbstractService { joint-iso-itu-t mhs(6) mts(3) modules(0)
                        mts-abstract-service(1) version-1999(1) }

        -- Object Identifiers

        id-ct-mts-access, id-ct-mts-forced-access, id-ot-mts, id-ot-mts-user,
        id-pt-administration, id-pt-delivery
                ----
                FROM MTSObjectIdentifiers { joint-iso-itu-t mhs(6) mts(3) modules(0)
                        object-identifiers(0) version-1999(1) }

        -- Operation Codes

        op-delivery-control, op-register
                ----
                FROM MTSAccessProtocol { joint-iso-itu-t mhs(6) protocols(0) modules(0)
                        mts-access-protocol(1) version-1999(1) }

        -- Upper Bounds

        ub-content-types, ub-labels-and-redirections
                ----
                FROM MTSUpperBounds { joint-iso-itu-t mhs(6) mts(3) modules(0) upper-bounds(3)
                        version-1999(1) };

--      Objects

mts-88 MHS-OBJECT ::= {
        INITIATES       { mts-forced-access-contract-88 }
        RESPONDS        { mts-access-contract-88 }
        ID              {id-ot-mts 88} }
```


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

```
mts-user-88 MHS-OBJECT ::= {
       INITIATES      { mts-access-contract-88 }
       RESPONDS       { mts-forced-access-contract-88 }
       ID             { id-ot-mts-user 88 } }
```

Figure C.1 – Abstract Syntax Definition of the 1988 MTS Abstract Service (Part 1 of 2)

```
-- Contracts

mts-access-contract-88 CONTRACT ::= {
       CONNECTION              mts-connect
       INITIATOR CONSUMER OF   { submission | delivery-88 | administration-88 }
       ID                      { id-ct-mts-access 88 } }

mts-forced-access-contract-88 CONTRACT ::= {
       CONNECTION              mts-connect
       RESPONDER CONSUMER OF   { submission | delivery-88 | administration-88 }
       ID                      { id-ct-mts-forced-access 88 } }

--      Ports

delivery-88 PORT ::= {
       OPERATIONS {operationObject1,...} /* This information object set has to be extensible
because it is used by Forward{} (as defined in ITU-T Rec. X.880) */
       CONSUMER INVOKES {delivery-control-88,...} -- This IOS needs to be extensible for
Forward{} of X.880--
       SUPPLIER INVOKES {message-delivery | report-delivery,...} -- This IOS needs to be
extensible for Forward{} of X.880--
       ID {id-pt-delivery 88}}

administration-88 PORT ::= {
       OPERATIONS {change-credentials,...} /* This information object set has to be extensible
because it is used by Forward{} (as defined in ITU-T Rec. X.880) */
       CONSUMER INVOKES {register-88,...} /* This information object set has to be extensible
because it is used by Forward{} (as defined in ITU-T Rec. X.880) */
       SUPPLIER INVOKES {operationObject1,...} /* This information object set has to be
extensible because it is used by Forward{} (as defined in ITU-T Rec. X.880) */
       ID {id-pt-administration 88}
  }

--      Delivery Port

delivery-control-88 ABSTRACT-OPERATION ::= {
       ARGUMENT          DeliveryControls88
       RESULT            Waiting
       ERRORS            { control-violates-registration | security-error }
       LINKED {operationObject1,...} /* This information object set has to be extensible
because it is used by Forward{} (as defined in ITU-T Rec. X.880) */
       INVOKE-PRIORITY   { 3 }
       CODE              op-delivery-control }

DeliveryControls88 ::= SET {
       COMPONENTS OF Controls (WITH COMPONENTS {
              ... ,
              permissible-encoded-information-types ABSENT } ),
       permissible-encoded-information-types-88 EncodedInformationTypes OPTIONAL }

--      Administration Port

register-88 ABSTRACT-OPERATION ::= {
       ARGUMENT          Register88
       RESULT            NULL
       ERRORS            { register-rejected }
       LINKED {operationObject1,...} /* This information object set has to be extensible
because it is used by Forward{} (as defined in ITU-T Rec. X.880) */
       INVOKE-PRIORITY   { 5 }
       CODE              op-register }
```


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

```
Register88 ::= SET {
       user-name UserName OPTIONAL,
       user-address [0] UserAddress OPTIONAL,
       deliverable-encoded-information-types EncodedInformationTypes OPTIONAL,
       deliverable-maximum-content-length [1] EXPLICIT ContentLength OPTIONAL,
       default-delivery-controls [2] EXPLICIT DefaultDeliveryControls OPTIONAL,
       deliverable-content-types [3] ContentTypes OPTIONAL,
       labels-and-redirections [4] SET SIZE (1..ub-labels-and-redirections) OF
              LabelAndRedirection OPTIONAL }

LabelAndRedirection ::= SET {
       user-security-label [0] UserSecurityLabel OPTIONAL,
       recipient-assigned-alternate-recipient [1] RecipientAssignedAlternateRecipient
                                                                    OPTIONAL }

UserSecurityLabel ::= SecurityLabel

END     -- of MTSAbstractService88
```

Figure C.1 – Abstract Syntax Definition of the 1988 MTS Abstract Service (Part 2 of 2)

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

Annex D

Differences between ISO/IEC 10021-4 and ITU-T Recommendation X.411

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

This annex identifies the technical differences between ITU-T Rec. X.411 and ISO/IEC 10021-4.

They are:

1. In ITU-T Rec. X.411, size constraints are applied to a number of protocol fields (see Annex B). In ISO/IEC 10021-4, the actual values of the constraints are not an integral part of the standard.

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

Annex E

Index

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

This annex provides an index to this Service Definition. It gives the number(s) of the page(s) on which each item in each of several categories is defined.

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

a) Abbreviations
b) Terms
c) Definitions of the MTS parameters
d) ASN.1 modules
e) ASN.1 information object classes
f) ASN.1 types
g) ASN.1 values

Abbreviations

- MTA 102
- MTS 4

Terms

- administration-port 5, 102
- application-context 104
- Cancel-deferred-delivery 6, 27
- Change-credentials 6, 54
- Criticality Mechanism 62
- Delivery-control 6, 45
- Delivery-control-88 171
- delivery-port 5, 102
- Extension Mechanism 62
- Message Transfer System 4, 102
- Message-delivery 6, 33
- Message-submission 6, 10
- Message-transfer 103
- message-transfer-agent 102
- MTA-bind 103, 104
- MTA-unbind 103
- MTS-bind 6, 7
- MTS-unbind 6, 9
- Probe-submission 6, 25
- Probe-transfer 103
- Register 6, 50
- Register-88 169
- Report-delivery 6, 37
- Report-transfer 103
- security-context 104
- Submission-control 6, 28
- submission-port 5, 102
- transfer-port 102

Definitions of the MTS parameters

- Actual-recipient-name 38
- Additional-information 113
- Algorithm-identifier 61
- alphabetic-character-loss (non-delivery-diagnostic-code) 41
- Alternate-recipient-allowed 11
- ambiguous-OR-name (non-delivery-diagnostic-code) 40
- Arrival-time 113
- asymmetric-token 60
- Authentication-error (bind-error) 10, 106
- authentication-failure-on-subject-message 49
- authentication-failure-on-subject-message (non-delivery-diagnostic-code) 43
- basic encoded-information-types 57

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

built-in content-type 20
built-in-domain-defined-attributes 57
built-in-encoded-information-types 58
built-in-standard-attributes 57
Busy (bind-error) 10, 106
Certificate 58
certificates 59
certificate-selector 8, 9, 105, 106
Certificate-selectors 23
Certificate-selectors-override 23
certification-path 59
Content 21
Content-confidentiality-algorithm-identifier 17
content-confidentiality-key 17
Content-correlator 21
Content-identifier 21
content-integrity-algorithm-identifier 18
Content-integrity-check 18
content-integrity-key 17
Content-length 26
Content-return-request 16
content-syntax-error (non-delivery-diagnostic-code) 41
content-too-long (non-delivery-diagnostic-code) 41
Content-type 20, 44
content-type-not-supported (non-delivery-diagnostic-code) 41
conversion-not-performed (non-delivery-reason-code) 40
Conversion-with-loss-prohibited 13
conversion-with-loss-prohibited (non-delivery-diagnostic-code) 41
Converted-encoded-information-types 36, 39
credentials 7, 9, 55, 104, 105
critical-for-delivery 63
critical-for-submission 63
critical-for-transfer 63
decryption-failed 49
decryption-failed (non-delivery-diagnostic-code) 43
decryption-key-unobtainable 49
decryption-key-unobtainable (non-delivery-diagnostic-code) 43
Default-delivery-control-arguments 54
deferred-delivery-not-performed (non-delivery-reason-code) 40
Deferred-delivery-time 14, 109
deliverable-class 51
Deliverable-classes 51
Deliverable-content-types 52, 170
Deliverable-encoded-information-types 170
Deliverable-maximum-content-length 52, 170
Deliverable-security-labels 53
directory-name 57
directory-operation-unsuccessful (non-delivery-reason-code) 40
Disclosure-of-other-recipients 13
DL-exempted-recipients 22
DL-expansion-failure (non-delivery-diagnostic-code) 41
DL-expansion-history 36
DL-expansion-prohibited 13
DL-expansion-prohibited (non-delivery-diagnostic-code) 41
DL-expansion-prohibited-by-security-policy (non-delivery-diagnostic-code) 42
domain-defined-attributes 57
double-envelope-creation-failure (non-delivery-diagnostic-code) 43
double-enveloping-message-restoring-failure (non-delivery-diagnostic-code) 43
edi-messaging (content-type) 21
Encoded-information-types 57
Encoded-information-types-constraints 51
encoded-information-types-unsupported (non-delivery-diagnostic-code) 41
encrypted-data 8, 9, 17, 60, 104, 105
Explicit-conversion 14, 110
extended content-type 21
extended-encoded-information-types 58
extension-domain-defined-attributes 57
extension-standard-attributes 57
external (content-type) 20
externally-defined encoded-information-type 58
failure-of-proof-of-message 49

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

failure-of-proof-of-message (non-delivery-diagnostic-code) 43
forbidden-alternate-recipient (non-delivery-diagnostic-code) 42
forbidden-user-security-label-register 56
Global-domain-identifier 57
implicit-conversion-not-subscribed (non-delivery-diagnostic-code) 41
Implicit-conversion-prohibited 13
implicit-conversion-prohibited (non-delivery-diagnostic-code) 41
improperly-specified-recipients 31
Inadequate-association-confidentiality (bind-error) 10, 106
incompatible-change-with-original-security-context 32, 49
incorrect-notification-type (non-delivery-diagnostic-code) 42
initiator-bind-token 8, 104
initiator-certificate 8, 104
Initiator-credentials 7, 104
Initiator-name 7, 104
inner-envelope (content-type) 21
integrity-failure-on-subject-message 49
integrity-failure-on-subject-message (non-delivery-diagnostic-code) 43
internal-trace-information 113
Internal-trace-information 109
interpersonal-messaging-1984 (content-type) 21
interpersonal-messaging-1988 (content-type) 21
invalid-arguments (non-delivery-diagnostic-code) 41
invalid-security-label 32, 49
invalid-security-label (non-delivery-diagnostic-code) 43
invalid-security-label-update 56
key-failure 49
key-failure (non-delivery-diagnostic-code) 43
Latest-delivery-time 14
line-too-long (non-delivery-diagnostic-code) 41
loop-detected (non-delivery-diagnostic-code) 40
mandatory-parameter-absence 32, 49, 56
mandatory-parameter-absence (non-delivery-diagnostic-code) 43
maximum-time-expired (non-delivery-diagnostic-code) 40
Message-delivery-identifier 34
Message-delivery-time 34, 39
Message-identifier 107
message-origin-authentication-algorithm-identifier 19
Message-origin-authentication-check 19
Message-security-label 19
message-sequence-number 17
Message-submission-identifier 24, 28
Message-submission-time 24
Messages-waiting 8, 9
Message-token 17
MTA-name 57
MTS-congestion (non-delivery-diagnostic-code) 40
MTS-identifier 56
multiple-information-loss (non-delivery-diagnostic-code) 41
Multiple-originator-certificates 22
New-credentials 55
no-bilateral-agreement (non-delivery-diagnostic-code) 41
no-DL-submit-permission (non-delivery-diagnostic-code) 41
Non-basic-parameters 58
Non-delivery-diagnostic-code 40
Non-delivery-reason-code 40
Notification-type 21
Old-credentials 55
operation-security-failure 32, 49, 56
operation-security-failure (non-delivery-diagnostic-code) 43
OR-address 57
Original-encoded-information-types 20
Originally-intended-recipient-name 35
Originally-specified-recipient-number 109
Originating-MTA-certificate 24
Originating-MTA-report-request 109
Originator-and-DL-expansion-history 38
Originator-certificate 16
Originator-name 11

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

Originator-report-request 16
Originator-requested-alternate-recipient 13
Originator-return-address 16
OR-name 57
Other-recipient-names 35
page-split (non-delivery-diagnostic-code) 41
password 7, 9, 55, 61, 104, 105
Per-domain-bilateral-information 107
Permissible-content-types 46
Permissible-encoded-information-types 46, 171
Permissible-lowest-priority 29, 46
Permissible-maximum-content-length 29, 47
Permissible-operations 29, 46
Permissible-security-context 29, 47
Physical-delivery-modes 15
physical-delivery-not-performed (non-delivery-reason-code) 40
Physical-delivery-report-request 16
Physical-forwarding-address 39
Physical-forwarding-address-request 15
Physical-forwarding-prohibited 14
Physical-rendition-attributes 15
physical-rendition-attributes-not-supported (non-delivery-diagnostic-code) 41
physical-rendition-not-performed (non-delivery-reason-code) 40
pictorial-symbol-loss (non-delivery-diagnostic-code) 41
Priority 13
privacy-mark 61
Probe-identifier 110
probe-origin-authentication-algorithm-identifier 26
Probe-origin-authentication-check 26
Probe-submission-identifier 27
Probe-submission-time 27
Proof-of-delivery 36
proof-of-delivery-algorithm-identifier 36
Proof-of-delivery-request 20
Proof-of-submission 24
proof-of-submission-algorithm-identifier 24
Proof-of-submission-request 20
protocol-violation (non-delivery-diagnostic-code) 41
punctuation-symbol-loss (non-delivery-diagnostic-code) 41
random-number 8, 9, 104, 105
recipient-assigned-alternate-recipient 53
Recipient-assigned-alternate-recipient 170
Recipient-assigned-redirections 53
Recipient-certificate 22, 36
Recipient-name 11
Recipient-number-for-advice 15
Recipient-reassignment-prohibited 12
recipient-reassignment-prohibited (non-delivery-diagnostic-code) 41
recipient-unavailable (non-delivery-diagnostic-code) 40
redirection-class 53
Redirection-history 35, 39
redirection-loop-detected (non-delivery-diagnostic-code) 41
redirection-prohibited 56
redirection-reason 35
refused-alternate-recipient-name 56
Registered-mail-type 15
Report-destination-name 112
Report-identifier 112
Reporting-DL-name 39
Reporting-MTA-certificate 43
report-origin-authentication-algorithm-identifier 44
Report-origin-authentication-check 44
repudiation-failure-of-message 49
repudiation-failure-of-message (non-delivery-diagnostic-code) 43
Requested-delivery-method 14
responder-bind-token 9, 105
responder-certificate 9, 105
Responder-credentials 9, 105
Responder-name 8, 105
Responsibility 109
Restrict 29, 46
Restricted-delivery 53
restricted-delivery (non-delivery-reason-code) 40

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

restriction 53
Retrieve-registrations 54
Returned-content 44
secure-messaging-error (non-delivery-diagnostic-code) 42
security-attributes 61
security-categories 61
security-classification 61
Security-context 8, 105
security-context-failure 32, 49
security-context-failure-message (non-delivery-diagnostic-code) 43
Security-label 60
security-policy-identifier 61
security-policy-violation 32, 49, 56
security-policy-violation (non-delivery-diagnostic-code) 42
security-problem 32, 48, 56
security-services-refusal 32, 49, 56
security-services-refusal (non-delivery-diagnostic-code) 42
Service-message 21
signed-data 8, 9, 17, 60, 104, 105
size-constraint-violation (non-delivery-diagnostic-code) 41
standard-attributes 57
Subject-identifier 113
Subject-intermediate-trace-information 113
subject-public-key 58
Subject-submission-identifier 38
Supplementary-information 39
This-recipient-name 34
Time 57
Token 60
token-decryption-failed 49
token-decryption-failed (non-delivery-diagnostic-code) 43
token-error 49
token-error (non-delivery-diagnostic-code) 43
token-type-identifier 60
too-many-recipients (non-delivery-diagnostic-code) 41
Trace-information 107, 113
transfer-attempts-limit-reached (non-delivery-diagnostic-code) 42
transfer-failure (non-delivery-reason-code) 40
transfer-failure-for-security-reason (non-delivery-reason-code) 40
Type-of-MTS-user 39
unable-to-complete-transfer (non-delivery-diagnostic-code) 42
unable-to-downgrade (non-delivery-diagnostic-code) 42
unable-to-transfer (non-delivery-reason-code) 40
Unacceptable-dialogue-mode 106
Unacceptable-dialogue-mode (bind-error) 10
Unacceptable-security-context (bind-error) 10, 106
unauthorised-DL-member (non-delivery-diagnostic-code) 42
unauthorised-dl-name 32
unauthorised-DL-name (non-delivery-diagnostic-code) 42
unauthorised-originally-intended-recipient-name 49
unauthorised-originally-intended-recipient-name (non-delivery-diagnostic-code) 43
unauthorised-originator-name 32, 49
unauthorised-originator-name (non-delivery-diagnostic-code) 43
unauthorised-recipient-name 32, 49
unauthorised-recipient-name (non-delivery-diagnostic-code) 43
unauthorised-security-label-update 56
unauthorised-user-name 56
undeliverable-mail-new-address-unknown (non-delivery-diagnostic-code) 42
undeliverable-mail-organization-expired (non-delivery-diagnostic-code) 42
undeliverable-mail-originator-prohibited-forwarding (non-delivery-diagnostic-code) 42
undeliverable-mail-physical-delivery-address-incomplete (non-delivery-diagnostic-code) 42
undeliverable-mail-physical-delivery-address-incorrect (non-delivery-diagnostic-code) 41
undeliverable-mail-physical-delivery-office-incorrect-or-invalid (non-delivery-diagnostic-code) 42
undeliverable-mail-recipient-changed-address-permanently (non-delivery-diagnostic-code) 42

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

undeliverable-mail-recipient-changed-address-temporarily (non-delivery-diagnostic-code) 42
undeliverable-mail-recipient-changed-temporary-address (non-delivery-diagnostic-code) 42
undeliverable-mail-recipient-deceased (non-delivery-diagnostic-code) 42
undeliverable-mail-recipient-did-not-claim (non-delivery-diagnostic-code) 42
undeliverable-mail-recipient-did-not-want-forwarding (non-delivery-diagnostic-code) 42
undeliverable-mail-recipient-refused-to-accept (non-delivery-diagnostic-code) 42
undeliverable-mail-recipient-unknown (non-delivery-diagnostic-code) 42
unidentified (content-type) 20
unknown-security-label 32, 49
unknown-security-label (non-delivery-diagnostic-code) 43
unrecognised-OR-name (non-delivery-diagnostic-code) 40
unreliable-system (non-delivery-diagnostic-code) 43
unsupported-algorithm-identifier 49
unsupported-algorithm-identifier (non-delivery-diagnostic-code) 43
unsupported-critical-function (non-delivery-diagnostic-code) 41
unsupported-security-policy 49
unsupported-security-policy (non-delivery-diagnostic-code) 43
User-address 51
User-name 51
User-security-labels 170
voice-messaging (content-type) 21
Waiting-content-types 30, 48
Waiting-encoded-information-types 30, 48
Waiting-messages 30, 47
Waiting-operations 30, 47

Definitions of the MTS parametersconversion-impractical
(non-delivery-diagnostic-code) 41

ASN.1 modules
MTAAbstractService 116
MTSAbstractService 65
MTSAbstractService88 172
MTSObjectIdentifiers 164
MTSUpperBounds 166

ASN.1 information object classes
ABSTRACT-ERROR 68
ABSTRACT-OPERATION 68
ADDITIONAL 121
ALGORITHM - see ISO/IEC 9594-8
BILATERAL 121
CONNECTION-PACKAGE - see ISO/IEC 13712-1
CONTRACT - see ISO/IEC 13712-1
ENCRYPTED { } - see ISO/IEC 9594-8
ERROR - see ISO/IEC 13712-1
EXTENSION 85
EXTENSION-ATTRIBUTE 93
IPMPerRecipientEnvelopeExtensions - see ISO/IEC 10021-7
MHS-OBJECT 66
OPERATION - see ISO/IEC 13712-1
OPERATION-PACKAGE - see ISO/IEC 13712-1
PORT 68
ROS-OBJECT-CLASS - see ISO/IEC 13712-1
SECURITY-CATEGORY 101
SIGNATURE { } - see ISO/IEC 9594-8
SIGNED { } - see ISO/IEC 9594-8
TOKEN 100
TOKEN-DATA 100

ASN.1 types
ActualRecipientName 82, 121
AdditionalActions 122
AdditionalInformation 121
AdministrationDomainName 93
AlgorithmIdentifier - see ISO/IEC 9594-8
ArrivalTime 123
AsymmetricToken 100
BilateralDomain 121
BindTokenEncryptedData 101
BindTokenSignedData 101
BuiltInContentType 81
BuiltInDomainDefinedAttribute 93

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

BuiltInDomainDefinedAttributes 93
BuiltInEncodedInformationTypes 98
BuiltInStandardAttributes 92
CancelDeferredDeliveryArgument 71
CancelDeferredDeliveryResult 71
CertificateAssertion - see ISO/IEC 9594-8
Certificates - see ISO/IEC 9594-8
CertificateSelectors 91
ChangeCredentialsArgument 76
CommonName 94
Content 92
ContentConfidentialityAlgorithmIdentifier 87
ContentCorrelator 88
ContentIdentifier 81
ContentIntegrityAlgorithmIdentifier 88
ContentIntegrityCheck 88
ContentLength 82
ContentType 81
ContentTypes 81
Controls 76
ConversionWithLossProhibited 86
ConvertedEncodedInformationTypes 82
CountryName 93
Credentials 70
Criticality 85
DefaultDeliveryControls 77
DeferredDeliveryTime 82
DeferredTime 123
DeliverableClass 77
DeliveredContentType 81
DeliveredOriginatorName 81
DeliveryControlArgument 74
DeliveryControlExtensions 74
DeliveryControlResult 75
DeliveryControlResultExtensions 75
DeliveryControls 75
DeliveryControls88 173
DeliveryFlags 82
DeliveryQueue 70
DeliveryReport 81
DLExemptedRecipients 91
DLExpansion 89
DLExpansionHistory 89
DLExpansionProhibited 85
DomainSuppliedInformation 122
EncodedInformationTypes 98
EncodedInformationTypesConstraints 77
EncryptionKey 101
ExactOrPattern 77
ExplicitConversion 82
ExtendedCertificate 91
ExtendedCertificates 91
ExtendedContentType 81
ExtendedEncodedInformationType 99
ExtendedEncodedInformationTypes 99
ExtendedNetworkAddress 98
ExtensionAttribute 93
ExtensionAttributes 93
ExtensionAttributeTable 94
ExtensionField 85
ExtensionORAddressComponents 96
ExtensionPhysicalDeliveryAddressComponents 96
ExtensionType 85
G3FacsimileNonBasicParameters 100
GlobalDomainIdentifier 92
ID 164
ImproperlySpecifiedRecipients 72
InitiatorCredentials 70
IntendedRecipientName 89
InternalAdditionalActions 122
InternalTraceInformation 122
InternalTraceInformationElement 122
LabelAndRedirection 174
LastTraceInformation 122
LatestDeliveryTime 86
LocalIdentifier 92
LocalPostalAttributes 97
Message 118
MessageClass 77
MessageClassExtensions 77

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

MessageDeliveryArgument 74
MessageDeliveryEnvelope 79
MessageDeliveryExtensions 80
MessageDeliveryIdentifier 82
MessageDeliveryResult 74
MessageDeliveryResultExtensions 74
MessageDeliveryTime 82
MessageIdentifier 120
MessageOriginAuthenticationAlgorithm Identifier 88
MessageOriginAuthenticationCheck 88
MessageOrProbeIdentifier 121
MessageSecurityLabel 88
MessageSubmissionArgument 71
MessageSubmissionEnvelope 78
MessageSubmissionIdentifier 73
MessageSubmissionResult 71
MessageSubmissionResultExtensions 71
MessageSubmissionTime 73
MessagesWaiting 70
MessageToken 87
MessageTokenEncryptedData 101
MessageTokenSignedData 101
MessageTransferEnvelope 118
MessageTransferExtensions 118
MTABindArgument 117
MTABindResult 117
MTAName 92
MTASuppliedInformation 122
MTSBindArgument 68
MTSBindExtensions 68
MTSBindResult 68
MTSBindResultExtensions 68
MTSIdentifier 92
Name - see ISO/IEC 9594-2
NetworkAddress 93
NonBasicParameters 99
NonDeliveryDiagnosticCode 83
NonDeliveryReasonCode 83
NonDeliveryReport 81
NumericUserIdentifier 93
ObjectName 70
Operations 74
ORAddress 92
ORAddressAndOptionalDirectoryName 92
ORAddressAndOrDirectoryName 92
OrganizationalUnitName 93
OrganizationalUnitNames 93
OrganizationName 93
OriginalEncodedInformationTypes 81
OriginallyIntendedRecipientName 82, 122
OriginallySpecifiedRecipientNumber 121
OriginatingMTACertificate 90
OriginatorAndDLExpansion 89
OriginatorAndDLExpansionHistory 89
OriginatorCertificate 87
OriginatorName 81, 120
OriginatorReportRequest 82
OriginatorRequestedAlternateRecipient 85, 122
OriginatorReturnAddress 87
ORName 92
OtherActions 123
OtherMessageDeliveryFields 79
OtherRecipientName 82
OtherRecipientNames 82
Password 70
PDSName 95
PDSParameter 98
PerDomainBilateralInformation 121
PerMessageIndicators 81
PerMessageSubmissionExtensions 78
PerMessageSubmissionFields 78
PerMessageTransferFields 118
PermissibleEncodedInformationTypes 76
PerProbeSubmissionExtensions 79
PerProbeSubmissionFields 79
PerProbeTransferFields 119
PerRecipientDeliveryReportFields 90
PerRecipientIndicators 121
PerRecipientMessageSubmissionExtensions 78

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

PerRecipientMessageSubmissionFields 78
PerRecipientMessageTransferExtensions 119
PerRecipientMessageTransferFields 118
PerRecipientNonDeliveryReportFields 90
PerRecipientProbeSubmissionExtensions 79
PerRecipientProbeSubmissionFields 79
PerRecipientProbeTransferExtensions 119
PerRecipientProbeTransferFields 119
PerRecipientReportDeliveryExtensions 80
PerRecipientReportDeliveryFields 80
PerRecipientReportFields 90
PerRecipientReportTransferExtensions 120
PerRecipientReportTransferFields 120
PerReportDeliveryFields 80
PerReportTransferFields 120
PersonalName 93
PhysicalDeliveryCountryName 96
PhysicalDeliveryModes 86
PhysicalDeliveryOfficeName 96
PhysicalDeliveryOfficeNumber 96
PhysicalDeliveryOrganizationName 96
PhysicalDeliveryPersonalName 96
PhysicalDeliveryReportRequest 87
PhysicalForwardingAddress 89
PhysicalForwardingAddressRequest 86
PhysicalForwardingProhibited 86
PhysicalRenditionAttributes 87
PostalCode 96
PosteRestanteAddress 97
PostOfficeBoxAddress 97
PresentationAddress - see ISO/IEC 9594-6
Priority 82
PrivacyMark 101
PrivateDomainIdentifier 92
PrivateDomainName 93
PrivateExtensions 85
Probe 118
ProbeIdentifier 121
ProbeOriginAuthenticationAlgorithmIdentifier 89
ProbeOriginAuthenticationCheck 89
ProbeResultExtensions 71
ProbeSubmissionArgument 71
ProbeSubmissionEnvelope 79
ProbeSubmissionIdentifier 73
ProbeSubmissionResult 71
ProbeSubmissionTime 73
ProbeTransferEnvelope 119
ProbeTransferExtensions 119
ProofOfDelivery 75
ProofOfDeliveryAlgorithmIdentifier 75
ProofOfDeliveryRequest 88
ProofOfSubmission 90
ProofOfSubmissionAlgorithmIdentifier 90
ProofOfSubmissionRequest 88
ProtectedPassword 70
PSAPAddress 77
RandomNumber 101
RecipientAssignedAlternateRecipient 77
RecipientCertificate 75
RecipientName 81, 121
RecipientNumberForAdvice 87
RecipientReassignmentProhibited 85
RecipientRedirection 77
Redirection 89
RedirectionClass 77
RedirectionHistory 89
RedirectionReason 89
Redirections 77
RefusalReason 75
RefusedArgument 75
RefusedOperation 75
Register88 174
RegisterArgument 76
RegisteredMailType 87
RegisterExtensions 76
RegisterResult 76
RegisterResultExtensions 76
RegistrationTypes 78
Report 118
ReportDeliveryArgument 74

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

ReportDeliveryEnvelope 80
ReportDeliveryExtensions 80
ReportDeliveryResult 74
ReportDeliveryResultExtensions 74
ReportDestinationName 121
ReportIdentifier 121
ReportingDLName 90
ReportingMTACertificate 90
ReportingMTAName 90
ReportOriginAuthenticationAlgorithmIdentifier 90
ReportOriginAuthenticationCheck 90
ReportTransferContent 120
ReportTransferContentExtensions 120
ReportTransferEnvelope 120
ReportTransferEnvelopeExtensions 120
ReportType 81
RequestedDeliveryMethod 86
ResponderCredentials 70
RestrictedDelivery 77
Restriction 77
RoutingAction 122
SecurityCategories 101
SecurityCategoriesTable 101
SecurityCategory 101
SecurityClassification 101
SecurityContext 70
SecurityLabel 101
SecurityPolicyIdentifier 101
SecurityProblem 72
StreetAddress 97
StrongCredentials 70
SubjectIdentifier 121
SubjectIntermediateTraceInformation 121
SubjectSubmissionIdentifier 82
SubmissionControlArgument 71
SubmissionControlResult 71
SubmissionControls 73
SupplementaryInformation 84
TeletexCommonName 94
TeletexDomainDefinedAttribute 98
TeletexDomainDefinedAttributes 98
TeletexNonBasicParameters 100
TeletexOrganizationalUnitName 95
TeletexOrganizationalUnitNames 95
TeletexOrganizationName 94
TeletexPersonalName 94
TerminalIdentifier 93
TerminalType 98
ThisRecipientName 82
Time 92
Token 100
TokenData 100
TokenDataTable 101
TokensTable 100
TraceInformation 122
TraceInformationElement 122
TypeOfMTSUser 82
UnformattedPostalAddress 97
UniquePostalName 97
UniversalCommonName 94
UniversalDomainDefinedAttribute 98
UniversalDomainDefinedAttributes 98
UniversalExtensionORAddressComponents 96
UniversalExtensionPhysicalDeliveryAddressComponents 96
UniversalLocalPostalAttributes 98
UniversalOrBMPString 95
UniversalOrganizationalUnitName 95
UniversalOrganizationalUnitNames 95
UniversalOrganizationName 94
UniversalPDSParameter 98
UniversalPersonalName 95
UniversalPhysicalDeliveryOfficeName 96
UniversalPhysicalDeliveryOfficeNumber 96
UniversalPhysicalDeliveryOrganizationName 96
UniversalPhysicalDeliveryPersonalName 96
UniversalPosteRestanteAddress 97
UniversalPostOfficeBoxAddress 97
UniversalStreetAddress 97
UniversalUnformattedPostalAddress 97

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

UniversalUniquePostalName 97
UserAddress 77
UserName 77
UserSecurityLabel 174
Waiting 73
WaitingMessages 74
X121Address 93

ASN.1 values

alias (RedirectionReason) 89
alphabetic-character-loss (NonDeliveryDiagnosticCode) 83
alternate-recipient-allowed 81
ambiguous-OR-name (NonDeliveryDiagnosticCode) 83
any-delivery-method (RequestedDeliveryMethod) 86
assemby-instructions-conflict-with-security-services (SecurityProblem) 72
asymmetric-token 100
authentication-error (Bind-Error) 69, 117
authentication-failure-on-subject-message (NonDeliveryDiagnosticCode) 83
authentication-failure-on-subject-message (SecurityProblem) 72
authentication-problem (SecurityProblem) 72
bind-token-encrypted-data 101
bind-token-signed-data 101
bit-5 81
bit-6 81
bureau-fax-delivery (PhysicalDeliveryModes) 86
busy (Bind-Error) 69, 117
cancel-deferred-delivery 71
certificate-selectors 91
certificate-selectors-override 91
change-credentials 76
common-name 94
confidential (SecurityClassification) 101
confidentiality-association-problem (SecurityProblem) 72
content-confidentiality-algorithm-identifier 87
content-correlator 88
content-integrity-check 88
content-return-request 81
content-syntax-error (NonDeliveryDiagnosticCode) 83
content-too-long (NonDeliveryDiagnosticCode) 83
content-type-not-supported (NonDeliveryDiagnosticCode) 83
control-violates-registration 75
conversion-impractical (NonDeliveryDiagnosticCode) 83
conversion-not-performed (NonDeliveryReasonCode) 83
conversion-with-loss-prohibited 85
conversion-with-loss-prohibited (NonDeliveryDiagnosticCode) 83
counter-collection (PhysicalDeliveryModes) 86
counter-collection-with-telephone-advice (PhysicalDeliveryModes) 86
counter-collection-with-teletex-advice (PhysicalDeliveryModes) 86
counter-collection-with-telex-advice (PhysicalDeliveryModes) 86
decryption-failed (NonDeliveryDiagnosticCode) 84
decryption-failed (SecurityProblem) 72
decryption-key-unobtainable (NonDeliveryDiagnosticCode) 84
decryption-key-unobtainable (SecurityProblem) 72
deferred-delivery-cancellation-rejected 72
deferred-delivery-not-performed (NonDeliveryReasonCode) 83
delivery-control 74
delivery-control-88 173
delivery-control-violated 75
directory-look-up (RedirectionReason) 89
directory-operation-unsuccessful (NonDeliveryReasonCode) 83
disclosure-of-other-recipients 81
dl (TypeOfMTSUser) 82
dl-exempted-recipients 91
dl-expansion-failure (NonDeliveryDiagnosticCode) 83
dl-expansion-history 89
dl-expansion-prohibited 85
dl-expansion-prohibited (NonDeliveryDiagnosticCode) 83

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

dl-expansion-prohibited-by-security-policy (NonDeliveryDiagnosticCode) 83

double-envelope-creation-failure (NonDeliveryDiagnosticCode) 84

double-enveloping-message-restoring-failure (NonDeliveryDiagnosticCode) 84

e163-4-address 98

element-of-service-not-subscribed 72

emptyUnbind - see ISO/IEC 13712-1

encoded-information-types-unsupported (NonDeliveryDiagnosticCode) 83

err-control-violates-registration - see ISO/IEC 10021-6

err-deferred-delivery-cancellation-rejected - see ISO/IEC 10021-6

err-delivery-control-violated - see ISO/IEC 10021-6

err-element-of-service-not-subscribed - see ISO/IEC 10021-6

err-inconsistent-request - see ISO/IEC 10021-6

err-message-submission-identifier-invalid - see ISO/IEC 10021-6

err-new-credentials-unacceptable - see ISO/IEC 10021-6

err-old-credentials-incorrectly-specified - see ISO/IEC 10021-6

err-operation-refused - see ISO/IEC 10021-6

err-originator-invalid - see ISO/IEC 10021-6

err-recipient-improperly-specified - see ISO/IEC 10021-6

err-register-rejected - see ISO/IEC 10021-6

err-remote-bind-error - see ISO/IEC 10021-6

err-security-error - see ISO/IEC 10021-6

err-submission-control-violated - see ISO/IEC 10021-6

err-unsupported-critical-function - see ISO/IEC 10021-6

express-mail (PhysicalDeliveryModes) 86

extended-network-address 98

extension-OR-address-components 96

extension-physical-delivery-address-components 96

failure-of-proof-of-message (NonDeliveryDiagnosticCode) 84

failure-of-proof-of-message (SecurityProblem) 72

forbidden-alternate-recipient (NonDeliveryDiagnosticCode) 83

forbidden-user-security-label-register (SecurityProblem) 72

forwarding-request - see ISO/IEC 10021-5

g3-facsimile (EncodedInformationType) 98

g3-facsimile-delivery (RequestedDeliveryMethod) 86

g4-class-1 (EncodedInformationType) 98

g4-facsimile-delivery (RequestedDeliveryMethod) 86

generation-qualifier 93, 94

given-name 93, 94

ia5-terminal-delivery (RequestedDeliveryMethod) 86

ia5-text (EncodedInformationType) 98

id-att 164

id-att-physicalRendition-basic 165

id-att-physicalRendition-no-cover-page 165

id-cont 164

id-cont-inner-envelope 165

id-cont-unidentified 165

id-cp 164

id-cp-mta-connect 165

id-cp-mts-connect 165

id-ct 164

id-ct-mta-transfer 165

id-ct-mts-access 165

id-ct-mts-forced-access 165

id-eit 164

id-eit-g3-facsimile 165

id-eit-g4-class-1 165

id-eit-ia5-text 165

id-eit-mixed-mode 165

id-eit-teletex 165

id-eit-unknown 165

id-eit-videotex 165

id-eit-voice 165

id-mod 164

id-mod-mta-abstract-service 164

id-mod-mts-abstract-service 164

id-mod-object-identifiers 164

id-mod-upper-bounds 164

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

id-mts 164
id-ot 164
id-ot-mta 164
id-ot-mts 164
id-ot-mts-user 164
id-pt 164
id-pt-administration 165
id-pt-delivery 165
id-pt-submission 165
id-pt-transfer 165
id-sa 164
id-sa-ms 165
id-sa-ua 165
id-tok 164
id-tok-asymmetricToken 165
implicit-conversion-allowed 82
implicit-conversion-not-subscribed (NonDeliveryDiagnosticCode) 83
implicit-conversion-prohibited 81, 82
implicit-conversion-prohibited (NonDeliveryDiagnosticCode) 83
inadequate-association-confidentiality (Bind-Error) 69, 117
incompatible-change-with-original-security-context (SecurityProblem) 72
inconsistent-request 72
incorrect-notification-type (NonDeliveryDiagnosticCode) 83
initials 93, 94
integrity-failure-on-subject-message (NonDeliveryDiagnosticCode) 84
integrity-failure-on-subject-message (SecurityProblem) 72
internal-trace-information 122
invalid-arguments (NonDeliveryDiagnosticCode) 83
invalid-security-label (NonDeliveryDiagnosticCode) 84
invalid-security-label (SecurityProblem) 72
invalid-security-label-update (SecurityProblem) 72
key-failure (NonDeliveryDiagnosticCode) 84
key-failure (SecurityProblem) 72
latest-delivery-time 86
line-too-long (NonDeliveryDiagnosticCode) 83
local-postal-attributes 97
loop-detected (NonDeliveryDiagnosticCode) 83
mandatory-parameter-absence (NonDeliveryDiagnosticCode) 84
mandatory-parameter-absence (SecurityProblem) 72
maximum-time-expired (NonDeliveryDiagnosticCode) 83
message-delivery 74
message-origin-authentication-check 88
message-security-label 88
message-submission 70
message-submission-identifier-invalid 72
message-token 87
message-token-encrypted-data 101
message-token-signed-data 101
message-transfer 118
mhs-delivery (RequestedDeliveryMethod) 86
mixed-mode (EncodedInformationType) 98
ms (TypeOfMTSUser) 82
mta 117
mta-bind 117
mta-bind-error 117
mta-connect 117
mta-transfer 117
mta-unbind 117
mts 66
mts-88 172
mts-access-contract 66
mts-access-contract-88 173
mts-bind 68
mts-bind-error 69
mts-congestion (NonDeliveryDiagnosticCode) 83
mts-connect 68
mts-forced-access-contract 67
mts-forced-access-contract-88 173
mts-unbind 69
mts-user 66
mts-user-88 173
multiple-information-loss (NonDeliveryDiagnosticCode) 83
multiple-originator-certificates 91

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

new-credentials-unacceptable 76
no-bilateral-agreement (NonDeliveryDiagnosticCode) 83
no-dl-submit-permission (NonDeliveryDiagnosticCode) 83
non-registered-mail (RegisteredMailType) 87
non-urgent (Priority) 82
normal (Priority) 82
old-credentials-incorrectly-specified 77
op-cancel-deferred-delivery - see ISO/IEC 10021-6
op-change-credentials - see ISO/IEC 10021-6
op-delivery-control - see ISO/IEC 10021-6
operation-refused 75
operation-security-failure (NonDeliveryDiagnosticCode) 84
operation-security-failure (SecurityProblem) 72
op-message-delivery - see ISO/IEC 10021-6
op-message-submission - see ISO/IEC 10021-6
op-probe-submission - see ISO/IEC 10021-6
op-register - see ISO/IEC 10021-6
op-report-delivery - see ISO/IEC 10021-6
op-submission-control - see ISO/IEC 10021-6
ordinary-mail (PhysicalDeliveryModes) 86
originating-MTA-certificate 90
originating-MTA-non-delivery-report 121
originating-MTA-report 121
originator-and-DL-expansion-history 89
originator-certificate 87
originator-invalid 72
originator-non-delivery-report 121
originator-report 121
originator-requested-alternate-recipient 85, 122
originator-requested-alternate-recipient (RedirectionReason) 89
originator-return-address 87
other (TypeOfMTSUser) 82
page-split (NonDeliveryDiagnosticCode) 83
pdau (TypeOfMTSUser) 82
pds-name 95
physical-delivery (RequestedDeliveryMethod) 86
physical-delivery-country-name 95
physical-delivery-modes 86
physical-delivery-not-performed (NonDeliveryReasonCode) 83
physical-delivery-office-name 96
physical-delivery-office-number 96
physical-delivery-organization-name 96
physical-delivery-personal-name 96
physical-delivery-report-request 87
physical-forwarding-address 89
physical-forwarding-address-request 86
physical-forwarding-prohibited 86
physical-recipient (TypeOfMTSUser) 82
physical-rendition-attributes 87
physical-rendition-attributes-not-supported (NonDeliveryDiagnosticCode) 83
physical-rendition-not-performed (NonDeliveryReasonCode) 83
pictorial-symbol-loss (NonDeliveryDiagnosticCode) 83
postal-code 96
poste-restante-address 97
post-office-box-address 97
private (TypeOfMTSUser) 82
private-extension 85
probe-origin-authentication-check 88
probe-submission 71
probe-transfer 118
proof-of-delivery 89
proof-of-delivery-request 88
proof-of-submission 90
proof-of-submission-request 88
protocol-violation (NonDeliveryDiagnosticCode) 83
psap-address 98
public (TypeOfMTSUser) 82
punctuation-symbol-loss (NonDeliveryDiagnosticCode) 83
recipient-assigned-alternate-recipient (RedirectionReason) 89
recipient-certificate 89
recipient-improperly-specified 72
recipient-MD-assigned-alternate-recipient (RedirectionReason) 89

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

recipient-number-for-advice 87
recipient-reassignment-prohibited 85
recipient-reassignment-prohibited (NonDeliveryDiagnosticCode) 83
recipient-unavailable (NonDeliveryDiagnosticCode) 83
redirection-history 89
redirection-loop-detected (NonDeliveryDiagnosticCode) 83
redirection-prohibited (SecurityProblem) 72
refused-alternate-recipient-name (SecurityProblem) 72
register 76
register-88 173
registered-mail (RegisteredMailType) 87
registered-mail-to-addressee-in-person (RegisteredMailType) 87
registered-mail-type 87
register-rejected 76
remote-bind-error 73
report-delivery 74
reporting-DL-name 90
reporting-MTA-certificate 90
reporting-MTA-name 90
report-origin-authentication-check 90
report-transfer 118
repudiation-failure-of-message (NonDeliveryDiagnosticCode) 84
repudiation-failure-of-message (SecurityProblem) 72
requested-delivery-method 86
responder-credentials-checking-problem (SecurityProblem) 72
responsibility 121
restricted (SecurityClassification) 101
restricted-delivery (NonDeliveryReasonCode) 83
return-of-notification-by-MHS (PhysicalDeliveryReportRequest) 87
return-of-notification-by-MHS-and-PDS (PhysicalDeliveryReportRequest) 87
return-of-notification-by-PDS (PhysicalDeliveryReportRequest) 87
return-of-undeliverable-mail-by-PDS (PhysicalDeliveryReportRequest) 87
secret (SecurityClassification) 101
secure-messaging-error (NonDeliveryDiagnosticCode) 83
security-context-failure (NonDeliveryDiagnosticCode) 84
security-context-failure (SecurityProblem) 72
security-context-problem (SecurityProblem) 72
security-error 72
security-policy-violation (NonDeliveryDiagnosticCode) 83
security-policy-violation (SecurityProblem) 72
security-services-refusal (NonDeliveryDiagnosticCode) 83
security-services-refusal (SecurityProblem) 72
service-message 81
size-constraint-violation (NonDeliveryDiagnosticCode) 83
special-delivery (PhysicalDeliveryModes) 86
standard-extension 85
street-address 97
submission-control 71
submission-control-violated 72
surname 93, 94
telephone-delivery (RequestedDeliveryMethod) 86
teletex (EncodedInformationType) 98
teletex-common-name 94
teletex-delivery (RequestedDeliveryMethod) 86
teletex-domain-defined-attributes 98
teletex-organizational-unit-names 95
teletex-organization-name 94
teletex-personal-name 94
telex-delivery (RequestedDeliveryMethod) 86
terminal-type 98
token-decryption-failed (NonDeliveryDiagnosticCode) 84
token-decryption-failed (SecurityProblem) 72
token-error (NonDeliveryDiagnosticCode) 84
token-error (SecurityProblem) 72
too-many-recipients (NonDeliveryDiagnosticCode) 83
top-secret (SecurityClassification) 101
trace-information 122

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

transfer 117
transfer-attempts-limit-reached (NonDeliveryDiagnosticCode) 83
transfer-failure (NonDeliveryReasonCode) 83
transfer-failure-for-security-reason (NonDeliveryReasonCode) 83
ub-additional-info 166
ub-bilateral-info 166
ub-bit-options 166
ub-built-in-content-type 166
ub-built-in-encoded-information-types 166
ub-certificates 166
ub-common-name-length 166
ub-content-correlator-length 166
ub-content-id-length 166
ub-content-length 166
ub-content-types 166
ub-country-name-alpha-length 166
ub-country-name-numeric-length 166
ub-deliverable-class 166
ub-diagnostic-codes 166
ub-dl-expansions 166
ub-domain-defined-attributes 166
ub-domain-defined-attribute-type-length 167
ub-domain-defined-attribute-value-length 167
ub-domain-name-length 167
ub-e163-4-number-length 167
ub-e163-4-sub-address-length 167
ub-encoded-information-types 167
ub-extension-attributes 167
ub-extension-types 167
ub-generation-qualifier-length 167
ub-given-name-length 167
ub-initials-length 167
ub-integer-options 167
ub-labels-and-redirections 167
ub-local-id-length 167
ub-mta-name-length 167
ub-mts-user-types 167
ub-numeric-user-id-length 167
ub-organizational-unit-name-length 167
ub-organizational-units 167
ub-organization-name-length 167
ub-orig-and-dl-expansions 167
ub-password-length 167
ub-pds-name-length 167
ub-pds-parameter-length 167
ub-pds-physical-address-lines 167
ub-postal-code-length 167
ub-privacy-mark-length 167
ub-queue-size 167
ub-reason-codes 167
ub-recipient-number-for-advice-length 167
ub-recipients 167
ub-redirection-classes 167
ub-redirections 167
ub-restrictions 168
ub-security-categories 168
ub-security-labels 168
ub-security-problems 168
ub-supplementary-info-length 168
ub-surname-length 168
ub-teletex-private-use-length 168
ub-terminal-id-length 168
ub-transfers 168
ub-tsap-id-length 168
ub-unformatted-address-length 168
ub-universal-generation-qualifier-length 168
ub-universal-given-name-length 168
ub-universal-initials-length 168
ub-universal-surname-length 168
ub-x121-address-length 168
unable-to-aggregate-security-labels (SecurityProblem) 72
unable-to-complete-transfer (NonDeliveryDiagnosticCode) 83
unable-to-downgrade (NonDeliveryDiagnosticCode) 83
unable-to-transfer (NonDeliveryReasonCode) 83
unacceptable-dialogue-mode (Bind-Error) 69, 117
unacceptable-security-context (Bind-Error) 69, 117

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

unauthorised-dl-member (NonDeliveryDiagnosticCode) 83
unauthorised-dl-name (NonDeliveryDiagnosticCode) 83
unauthorised-dl-name (SecurityProblem) 72
unauthorised-entry-class (SecurityProblem) 72
unauthorised-originally-intended-recipient-name (SecurityProblem) 72
unauthorised-originally-intended-recipient-name (NonDeliveryDiagnosticCode) 83
unauthorised-originator-name (NonDeliveryDiagnosticCode) 83
unauthorised-originator-name (SecurityProblem) 72
unauthorised-recipient-name (NonDeliveryDiagnosticCode) 83
unauthorised-recipient-name (SecurityProblem) 72
unauthorised-security-label (SecurityProblem) 72
unauthorised-user-name (SecurityProblem) 72
unclassified (SecurityClassification) 101
undeliverable-mail-new-address-unknown (NonDeliveryDiagnosticCode) 83
undeliverable-mail-organization-expired (NonDeliveryDiagnosticCode) 83
undeliverable-mail-originator-prohibited-forwarding (NonDeliveryDiagnosticCode) 83
undeliverable-mail-physical-delivery-address-incomplete (NonDeliveryDiagnosticCode) 83
undeliverable-mail-physical-delivery-address-incorrect (NonDeliveryDiagnosticCode) 83
undeliverable-mail-physical-delivery-office-incorrect-or-invalid (NonDeliveryDiagnosticCode) 83
undeliverable-mail-recipient-changed-address-permanently (NonDeliveryDiagnosticCode) 83
undeliverable-mail-recipient-changed-address-temporarily (NonDeliveryDiagnosticCode) 83
undeliverable-mail-recipient-changed-temporary-address (NonDeliveryDiagnosticCode) 83
undeliverable-mail-recipient-deceased (NonDeliveryDiagnosticCode) 83
undeliverable-mail-recipient-did-not-claim (NonDeliveryDiagnosticCode) 83
undeliverable-mail-recipient-did-not-want-forwarding (NonDeliveryDiagnosticCode) 83
undeliverable-mail-recipient-refused-to-accept (NonDeliveryDiagnosticCode) 83
undeliverable-mail-recipient-unknown (NonDeliveryDiagnosticCode) 83
unformatted-postal-address 97
unique-postal-name 97
universal-domain-defined-attributes 98
universal-extension-OR-address-components 96
universal-extension-physical-delivery-address-components 96
universal-local-postal-attributes 98
universal-organizational-unit-names 95
universal-physical-delivery-office-name 96
universal-physical-delivery-office-number 96
universal-physical-delivery-organization-name 96
universal-physical-delivery-personal-name 96
universal-poste-restante-address 97
universal-post-office-box-address 97
universal-street-address 97
universal-unformatted-postal-address 97
universal-unique-postal-name 97
unknown (EncodedInformationType) 98
unknown-security-label (NonDeliveryDiagnosticCode) 84
unknown-security-label (SecurityProblem) 72
unmarked (SecurityClassification) 101
unrecognised-OR-name (NonDeliveryDiagnosticCode) 83
unreliable-system (NonDeliveryDiagnosticCode) 83
unsupported-algorithm-identifier (NonDeliveryDiagnosticCode) 84
unsupported-algorithm-identifier (SecurityProblem) 72
unsupported-critical-function 72
unsupported-critical-function (NonDeliveryDiagnosticCode) 83
unsupported-security-policy (NonDeliveryDiagnosticCode) 84
unsupported-security-policy (SecurityProblem) 72
urgent (Priority) 82
videotex (EncodedInformationType) 98
videotex-delivery (RequestedDeliveryMethod) 86
voice (EncodedInformationType) 98

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

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

ICS 35.240.20

Price based on 192 pages

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