

INTERNATIONAL STANDARD

ISO/IEC 10021-4

First edition
1990-12-01

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

Part 4: Message Transfer System: Abstract Service Definition and Procedures

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

*Partie 4: Système de transfert de message: Procédures et définition de service
abstrait*



Reference number
ISO/IEC 10021-4 : 1990 (E)



Documents

Document Sharing Hub

Contents

Foreword xi

Introduction xii

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

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

Section two - Message Transfer System Abstract Service 5

6 Message Transfer System Model 5

7 Message Transfer System Abstract Service Overview 6

7.1 MTS Bind and Unbind..... 7

7.2 Submission Port..... 7

7.3 Delivery Port..... 7

7.4 Administration Port 7

8 Message Transfer System Abstract Service Definition..... 8

8.1 MTS-bind and MTS-unbind..... 8

8.1.1 Abstract-bind and Abstract-unbind 8

8.1.1.1 MTS-bind 8

8.1.1.1.1 Arguments 8

8.1.1.1.1.1 Initiator-name 9

8.1.1.1.1.2 Initiator-credentials 9

8.1.1.1.1.3 Security-context 10

8.1.1.1.1.4 Messages-waiting 10

8.1.1.1.2 Results..... 10

8.1.1.1.2.1 Responder-name 10

8.1.1.1.2.2 Responder-credentials 11

8.1.1.1.2.3 Messages-waiting 11

8.1.1.1.3 Bind-errors 11

8.1.1.2	MTS-unbind	11
8.1.1.2.1	Arguments	11
8.1.1.2.2	Results	11
8.1.1.2.3	Unbind-errors	11
8.1.2	Bind-errors	12
8.1.2.1	Authentication-error	12
8.1.2.2	Busy	12
8.1.2.3	Unacceptable-dialogue-mode	12
8.1.2.4	Unacceptable-security-context	12
8.2	Submission Port	12
8.2.1	Abstract-operations	12
8.2.1.1	Message-submission	13
8.2.1.1.1	Arguments	13
8.2.1.1.1.1	Originator-name	14
8.2.1.1.1.2	Recipient-name	14
8.2.1.1.1.3	Alternate-recipient-allowed	15
8.2.1.1.1.4	Recipient-reassignment-prohibited	15
8.2.1.1.1.5	Originator-requested-alternate-recipient	15
8.2.1.1.1.6	DL-expansion-prohibited	16
8.2.1.1.1.7	Disclosure-of-recipients	16
8.2.1.1.1.8	Priority	16
8.2.1.1.1.9	Implicit-conversion-prohibited	16
8.2.1.1.1.10	Conversion-with-loss-prohibited	16
8.2.1.1.1.11	Explicit-conversion	17
8.2.1.1.1.12	Deferred-delivery-time	17
8.2.1.1.1.13	Latest-delivery-time	17
8.2.1.1.1.14	Requested-delivery-method	17
8.2.1.1.1.15	Physical-forwarding-prohibited	18
8.2.1.1.1.16	Physical-forwarding-address-request	18
8.2.1.1.1.17	Physical-delivery-modes	18
8.2.1.1.1.18	Registered-mail-type	19
8.2.1.1.1.19	Recipient-number-for-advice	19
8.2.1.1.1.20	Physical-rendition-attributes	19
8.2.1.1.1.21	Originator-return-address	19
8.2.1.1.1.22	Originator-report-request	20
8.2.1.1.1.23	Content-return-request	20
8.2.1.1.1.24	Physical-delivery-report-request	20
8.2.1.1.1.25	Originator-certificate	20
8.2.1.1.1.26	Message-token	21
8.2.1.1.1.27	Content-confidentiality-algorithm-identifier	21
8.2.1.1.1.28	Content-integrity-check	22
8.2.1.1.1.29	Message-origin-authentication-check	22
8.2.1.1.1.30	Message-security-label	23
8.2.1.1.1.31	Proof-of-submission-request	24
8.2.1.1.1.32	Proof-of-delivery-request	24
8.2.1.1.1.33	Original-encoded-information-types	24
8.2.1.1.1.34	Content-type	24
8.2.1.1.1.35	Content-identifier	25
8.2.1.1.1.36	Content-correlator	25
8.2.1.1.1.37	Content	25
8.2.1.1.2	Results	25
8.2.1.1.2.1	Message-submission-identifier	26
8.2.1.1.2.2	Message-submission-time	26
8.2.1.1.2.3	Originating-MTA-certificate	26
8.2.1.1.2.4	Proof-of-submission	26
8.2.1.1.3	Abstract-errors	27
8.2.1.2	Probe-submission	27
8.2.1.2.1	Arguments	28
8.2.1.2.1.1	Probe-origin-authentication-check	29
8.2.1.2.1.2	Content-length	29
8.2.1.2.2	Results	29
8.2.1.2.2.1	Probe-submission-identifier	30
8.2.1.2.2.2	Probe-submission-time	30
8.2.1.2.3	Abstract-errors	30
8.2.1.3	Cancel-deferred-delivery	30

	8.2.1.3.1	Arguments	31
	8.2.1.3.1.1	Message-submission-identifier.....	31
	8.2.1.3.2	Results.....	31
	8.2.1.3.3	Abstract-errors.....	31
8.2.1.4	Submission-control.....		32
	8.2.1.4.1	Arguments	32
	8.2.1.4.1.1	Restrict	32
	8.2.1.4.1.2	Permissible-operations.....	32
	8.2.1.4.1.3	Permissible-lowest-priority	33
	8.2.1.4.1.4	Permissible-maximum-content-length	33
	8.2.1.4.1.5	Permissible-security-context.....	33
	8.2.1.4.2	Results.....	33
	8.2.1.4.2.1	Waiting-operations.....	34
	8.2.1.4.2.2	Waiting-messages.....	34
	8.2.1.4.2.3	Waiting-encoded-information-types.....	34
	8.2.1.4.2.4	Waiting-content-types	35
	8.2.1.4.3	Abstract-errors	35
8.2.2	Abstract-errors		35
	8.2.2.1	Submission-control-violated.....	35
	8.2.2.2	Element-of-service-not-subscribed.....	36
	8.2.2.3	Deferred-delivery-cancellation-rejected.....	36
	8.2.2.4	Originator-invalid	36
	8.2.2.5	Recipient-improperly-specified.....	36
	8.2.2.6	Message-submission-identifier-invalid	36
	8.2.2.7	Inconsistent-request.....	36
	8.2.2.8	Security-error.....	36
	8.2.2.9	Unsupported-critical-function.....	37
	8.2.2.10	Remote-bind-error	37
8.3	Delivery Port.....		37
8.3.1	Abstract-operations.....		37
	8.3.1.1	Message-delivery	37
	8.3.1.1.1	Arguments	37
	8.3.1.1.1.1	Message-delivery-identifier	39
	8.3.1.1.1.2	Message-delivery-time	39
	8.3.1.1.1.3	This-recipient-name	39
	8.3.1.1.1.4	Intended-recipient-name.....	40
	8.3.1.1.1.5	Redirection-reason.....	40
	8.3.1.1.1.6	Other-recipient-names	40
	8.3.1.1.1.7	DL-expansion-history	40
	8.3.1.1.1.8	Converted-encoded-information-types	40
	8.3.1.1.2	Results.....	41
	8.3.1.1.2.1	Recipient-certificate.....	41
	8.3.1.1.2.2	Proof-of-delivery	41
	8.3.1.1.3	Abstract-errors	42
8.3.1.2	Report-delivery.....		42
	8.3.1.2.1	Arguments	42
	8.3.1.2.1.1	Subject-submission-identifier.....	44
	8.3.1.2.1.2	Actual-recipient-name	44
	8.3.1.2.1.3	Originator-and-DL-expansion-history.....	44
	8.3.1.2.1.4	Reporting-DL-name.....	44
	8.3.1.2.1.5	Converted-encoded-information-types	44
	8.3.1.2.1.6	Supplementary-information	44
	8.3.1.2.1.7	Physical-forwarding-address.....	45
	8.3.1.2.1.8	Message-delivery-time	45
	8.3.1.2.1.9	Type-of-MTS-user	45
	8.3.1.2.1.10	Non-delivery-reason-code	45
	8.3.1.2.1.11	Non-delivery-diagnostic-code	46
	8.3.1.2.1.12	Reporting-MTA-certificate	49
	8.3.1.2.1.13	Report-origin-authentication-check.....	49
	8.3.1.2.1.14	Returned-content.....	50
	8.3.1.2.2	Results.....	50
	8.3.1.2.3	Abstract-errors	50
8.3.1.3	Delivery-control.....		50
	8.3.1.3.1	Arguments	51
	8.3.1.3.1.1	Restrict	51

	8.3.1.3.1.2	Permissible-operations	51
	8.3.1.3.1.3	Permissible-lowest-priority	52
	8.3.1.3.1.4	Permissible-encoded-information-types	52
	8.3.1.3.1.5	Permissible-content-types	52
	8.3.1.3.1.6	Permissible-maximum-content-length	52
	8.3.1.3.1.7	Permissible-security-context	53
	8.3.1.3.2	Results	53
	8.3.1.3.2.1	Waiting-operations	53
	8.3.1.3.2.2	Waiting-messages	53
	8.3.1.3.2.3	Waiting-encoded-information-types	54
	8.3.1.3.2.4	Waiting-content-types	54
	8.3.1.3.3	Abstract-errors	54
8.3.2	Abstract-errors		54
	8.3.2.1	Delivery-control-violated	55
	8.3.2.2	Control-violates-registration	55
	8.3.2.3	Security-error	55
	8.3.2.4	Unsupported-critical-function	55
8.4	Administration Port		55
	8.4.1	Abstract-operations	55
	8.4.1.1	Register	55
	8.4.1.1.1	Arguments	56
	8.4.1.1.1.1	User-name	56
	8.4.1.1.1.2	User-address	56
	8.4.1.1.1.3	Deliverable-encoded-information-types	57
	8.4.1.1.1.4	Deliverable-content-types	57
	8.4.1.1.1.5	Deliverable-maximum-content-length	57
	8.4.1.1.1.6	Recipient-assigned-alternate-recipient	57
	8.4.1.1.1.7	User-security-labels	58
	8.4.1.1.1.8	Default Delivery Control Arguments	58
	8.4.1.1.2	Results	58
	8.4.1.1.3	Abstract-errors	58
	8.4.1.2	Change-credentials	59
	8.4.1.2.1	Arguments	59
	8.4.1.2.1.1	Old-credentials	59
	8.4.1.2.1.2	New-credentials	59
	8.4.1.2.2	Results	59
	8.4.1.2.3	Abstract-errors	60
8.4.2	Abstract-errors		60
	8.4.2.1	Register-rejected	60
	8.4.2.2	New-credentials-unacceptable	60
	8.4.2.3	Old-credentials-incorrectly-specified	60
8.5	Common Parameter Types		60
	8.5.1	MTS-identifier	61
	8.5.2	Global-domain-identifier	61
	8.5.3	MTA-name	61
	8.5.4	Time	61
	8.5.5	OR-name	61
	8.5.6	Encoded-information-types	62
	8.5.7	Certificate	63
	8.5.8	Token	64
	8.5.9	Security-label	64
	8.5.10	Algorithm-identifier	65
9	Message Transfer System Abstract Syntax Definition		65
	9.1	Criticality Mechanism	66

Section three - Message Transfer Agent Abstract Service 94

10 Refined Message Transfer System Model 94

11 Message Transfer Agent Abstract Service Overview..... 95

11.1 MTA-bind and MTA-unbind..... 95

11.2 Transfer Port Abstract-operations 95

12 Message Transfer Agent Abstract Service Definition 96

12.1 MTA-bind and MTA-unbind..... 96

12.1.1 Abstract-bind and Abstract-unbind..... 96

12.1.1.1 MTA-bind..... 96

12.1.1.1.1 Arguments 96

12.1.1.1.1.1 Initiator-name 97

12.1.1.1.1.2 Initiator-credentials 97

12.1.1.1.1.3 Security-context 97

12.1.1.1.2 Results..... 98

12.1.1.1.2.1 Responder-name 98

12.1.1.1.2.2 Responder-credentials 98

12.1.1.1.3 Bind-errors 98

12.1.1.2 MTA-unbind..... 98

12.1.1.2.1 Arguments 99

12.1.1.2.2 Results..... 99

12.1.1.2.3 Unbind-errors 99

12.1.2 Bind-errors 99

12.1.2.1 Authentication-error..... 99

12.1.2.2 Busy 99

12.1.2.3 Unacceptable-dialogue-mode..... 99

12.1.2.4 Unacceptable-security-context 99

12.2 Transfer Port..... 100

12.2.1 Abstract-operations..... 100

12.2.1.1 Message-transfer..... 100

12.2.1.1.1 Arguments 100

12.2.1.1.1.1 Message-identifier 102

12.2.1.1.1.2 Per-domain-bilateral-information 102

12.2.1.1.1.3 Trace-information..... 102

12.2.1.1.1.4 Internal-trace-information 103

12.2.1.1.1.5 Originally-specified-recipient-number 103

12.2.1.1.1.6 Responsibility..... 103

12.2.1.1.1.7 Deferred-delivery-time 103

12.2.1.1.1.8 Originating-MTA-report-request 103

12.2.1.1.2 Results..... 104

12.2.1.1.3 Abstract-errors 104

12.2.1.2 Probe-transfer 104

12.2.1.2.1 Arguments 104

12.2.1.2.1.1 Probe-identifier 105

12.2.1.2.2 Results..... 106

12.2.1.2.3 Abstract-errors 106

12.2.1.3 Report-transfer 106

12.2.1.3.1 Arguments 106

12.2.1.3.1.1 Report-identifier 107

12.2.1.3.1.2 Report-destination-name 108

12.2.1.3.1.3 Subject-identifier..... 108

12.2.1.3.1.4 Subject-intermediate-trace-information 108

12.2.1.3.1.5 Arrival-time 108

12.2.1.3.1.6 Additional-information 108

12.2.1.3.2 Results..... 108

12.2.1.3.3 Abstract-errors 108

12.2.2 Abstract-errors 108

12.3 Common Parameter Types 108

12.3.1 Trace-information and internal-trace-information 109

13 Message Transfer Agent Abstract Syntax Definition..... 110

Section four - Procedures for Distributed Operation of the MTS 119

14 Procedures for Distributed Operation of the MTS..... 119

14.1 Overview of the MTA Model..... 119

14.1.1 Organization and Modelling Technique..... 119

14.2 Deferred Delivery Module 122

14.2.1 Deferred Delivery Procedure 122

14.3 Main Module 123

14.3.1	Control Procedure	126
14.3.2	Front-end Procedure	128
14.3.3	Routing-and-conversion-decision Procedure	129
14.3.4	Routing-decision Procedure	130
14.3.5	Conversion-decision Procedure	132
14.3.6	Error-processing Procedure	133
14.3.7	Redirection Procedure	135
14.3.8	Splitter Procedure	135
14.3.9	Conversion-procedure	137
14.3.10	Distribution-list-expansion Procedure	137
14.3.11	Loop Detection and Routing Algorithm	139
14.4	Report Module	140
14.4.1	Control Procedure	141
14.4.2	Report-front-end Procedure	142
14.4.3	Report-generation Procedure	143
14.4.4	Report-routing Procedure	143
14.5	MTS-bind and MTS-unbind	145
14.5.1	MTS-user initiated MTS-bind Procedure	145
14.5.2	MTS-user initiated MTS-unbind Procedure	146
14.5.3	MTA initiated MTS-bind Procedure	146
14.5.4	MTA initiated MTS-unbind Procedure	147
14.6	Submission Port	147
14.6.1	Message-submission Procedure	147
14.6.2	Probe-submission Procedure	149
14.6.3	Cancel-deferred-delivery Procedure	150
14.6.4	Submission-control Procedure	151
14.7	Delivery Port	151
14.7.1	Message-delivery Procedure	151
14.7.2	Probe-delivery-test Procedure	154
14.7.3	Report-delivery Procedure	154
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	158
14.9	MTA-bind and MTA-unbind	158
14.9.1	MTA-bind-in Procedure	158
14.9.2	MTA-unbind-in Procedure	159
14.9.3	MTA-bind-out Procedure	159
14.9.4	MTA-unbind-out Procedure	160
14.10	Transfer Port	160
14.10.1	Message-in Procedure	160
14.10.2	Probe-in Procedure	161
14.10.3	Report-in Procedure	161
14.10.4	Message-out Procedure	162
14.10.5	Probe-out Procedure	163
14.10.6	Report-out Procedure	163

Annexes 165

A	Reference Definition of MTS Object Identifiers	165
B	Reference Definition of MTS Parameter Upper Bounds	168
C	Differences between ISO/IEC 10021-4 and CCITT Recommendation X.411	172
D	Index	173

List of Figures

1 Message Transfer System Model 6

2 Abstract Syntax Definition of the MTS Abstract Service 68-93

3 Refined Message Transfer System Model.....95

4 Abstract Syntax Definition of the MTA Abstract Service..... 112-118

5 Ports and Modules of an MTA 121

6 Relationship of Internal and External Modules 122

7 Organisation of Procedures within the Main Module 125

8 Information Flow within the Main Module 126

9 Organisation of Procedures within Routing and Conversion Decision Procedure..... 130

10 Organisation of Procedures within the Report Module..... 140

11 Information Flow within the Report Module..... 142

A.1 Abstract Syntax Definition of the MTS Object Identifiers..... 166-167

B.1 Abstract Syntax Definition of MTS Upper Bounds..... 169-171

List of Tables

1 MTS-bind Arguments..... 9

2 MTS-bind Results..... 10

3 Message-submission Arguments..... 13-14

4 Combined Effect of Conversion Arguments 17

5 Message-submission Results..... 26

6 Message-submission Abstract-errors 27

7 Probe-submission Arguments 28-29

8 Probe-submission Results 30

9 Probe-submission Abstract-errors 30

10 Cancel-deferred-delivery Arguments 31

11 Cancel-deferred-delivery Abstract-errors..... 31

12 Submission-control Arguments..... 32

13 Submission-control Results..... 34

14 Submission-control Abstract-errors 35

15 Message-delivery Arguments 38-39

16 Message-delivery Results 41

17 Message-delivery Abstract-errors 42

18 Report-delivery Arguments 43

19 Report-delivery Abstract-errors 50

20 Delivery-control Arguments 51

21 Delivery-control Results 53

22 Delivery-control Abstract-errors 54

23 Register Arguments..... 56

24 Register Abstract-errors 58

25 Change-credentials Arguments..... 59

26 Change-credentials Abstract-errors..... 60

27 MTA-bind Arguments 97

28 MTA-bind Results 98

29 Message-transfer Arguments 100-102

30 Probe-transfer Arguments..... 104-105

31 Report-transfer Arguments 106-107

Foreword

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

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

International Standard ISO/IEC 10021-4 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*.

ISO/IEC 10021-4 consists of the following parts, under the general title: *Information technology — Text Communication — Message-Oriented Text Interchange Systems (MOTIS)* —

- *Part 1: System and Service Overview*
- *Part 2: Overall Architecture*
- *Part 3: Abstract Service Definition Conventions*
- *Part 4: Message Transfer System: Abstract Service Definition and Procedures*
- *Part 5: Message Store: Abstract Service Definition*
- *Part 6: Protocol Specifications*
- *Part 7: Interpersonal Messaging System*

Annex A forms an integral part of this part of ISO/IEC 10021. Annexes B, C and D are for information only.

Introduction

This part of ISO/IEC 10021 is one of a number of parts of ISO/IEC 10021 (the International Standards for Message-Oriented Text Interchange Systems (MOTIS)).

MOTIS 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 International Standard was developed jointly by CCITT and ISO/IEC. The equivalent CCITT document is CCITT Recommendation X.411.

**Information technology - Text Communication -
Message-Oriented Text Interchange Systems (MOTIS) -
Part 4 : Message Transfer System: Abstract Service Definition and
Procedures**

Section one - Introduction

1 Scope

This part of ISO/IEC 10021 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.

ISO/IEC 10021-2 identifies the other International Standards which define other aspects of Message Handling Systems.

Access to the MTS Abstract Service defined in this part of ISO/IEC 10021 may be provided by the MTS Access Protocol (P3) defined in ISO/IEC 10021-6. The distributed operation of the MTS defined in this part of ISO/IEC 10021 may be provided by the use of the MTS Transfer Protocol (P1) also defined in ISO/IEC 10021-6.

Section two of this part of ISO/IEC 10021 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 part of ISO/IEC 10021 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 part of ISO/IEC 10021 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 part of ISO/IEC 10021.

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 CCITT Recommendation X.411.

Annex C identifies the technical differences between the ISO/IEC and CCITT versions of CCITT Recommendation X.411 and this part of ISO/IEC 10021.

Annex D provides an index to this part of ISO/IEC 10021, categorised into: definitions of the MTS parameters; Abbreviations; Terms; ASN.1 modules; ASN.1 macros; ASN.1 types; and ASN.1 values.

2 Normative references

The following standards contain provisions which, through reference in this text, constitute provisions of this part of ISO/IEC 10021. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this part of ISO/IEC 10021 are

encouraged to investigate the possibility of applying the most recent editions of the standards listed below. Members of ISO and IEC maintain registers of currently valid International Standards.

2.1 Open Systems Interconnection

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

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

2.2 Message Handling Systems

This part of ISO/IEC 10021 cites the following Message Handling System specifications:

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

Part 1: Service and system overview.

Part 2: Overall architecture.

Part 3: Abstract service definition conventions.

Part 5: Message store : Abstract service definition.

Part 6: Protocol specifications.

Part 7: Interpersonal messaging system.

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

2.3 Directory Systems

This part of ISO/IEC 10021 cites the following Directory System specifications:

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

Part 1: Overview of concepts, models, and services.

Part 2: Models.

Part 3: Abstract service definition.

Part 4: Procedures for distributed operation.

Part 5: Protocol specifications.

Part 6: Selected attribute types.

Part 7: Selected object classes.

Part 8: Authentication framework.

2.4 Country Codes

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

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

3 Definitions

For the purposes of this part of ISO/IEC 10021 the definitions given in ISO/IEC 10021-2 apply.

4 Abbreviations

For the purposes of this part of ISO/IEC 10021 the abbreviations given in ISO/IEC 10021-2 apply.

5 Conventions

This International Standard uses the descriptive conventions described below.

5.1 Terms

Throughout this part of ISO/IEC 10021 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. In clauses 8 and 12, the names and values of the parameters of the MTS Abstract Service and the MTA Abstract Service 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 as defined by this International Standard.

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 part of ISO/IEC 10021 defines the abstract-syntax of the MTS Abstract Service and the MTA Abstract Service using the abstract syntax notation (ASN.1) defined in ISO 8824, and the abstract service definition conventions defined in ISO/IEC 10021-3.

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.

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 (eg the MTS) is usually regarded as being the *supplier*, and the user object (eg an MTS-user object) is usually regarded as being the *consumer*.

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

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

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

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

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

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

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

Figure 1 models the Message Transfer System (MTS).

Clause 7 provides an overview of the MTS Abstract Service.

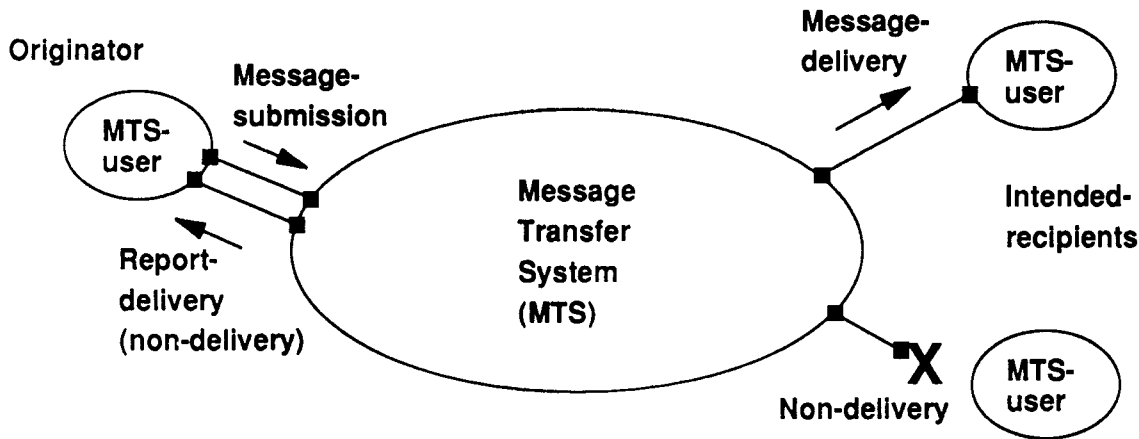


Figure 1
Message Transfer System Model

7 Message Transfer System Abstract Service Overview

This part of ISO/IEC 10021 defines the following services that comprise the MTS Abstract Service:

MTS Bind and Unbind

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

Submission Port Abstract Operations

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

Delivery Port Abstract Operations

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

Administration Port Abstract Operations

- j) Register
- k) Change-credentials.

7.1 MTS Bind and Unbind

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

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

7.2 Submission Port

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

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

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

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

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

7.3 Delivery Port

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

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

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

7.4 Administration Port

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

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

8 Message Transfer System Abstract Service Definition

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

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

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

8.1 MTS-bind and MTS-unbind

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

8.1.1 Abstract-bind and Abstract-unbind

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

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

8.1.1.1 MTS-bind

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

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

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

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

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

8.1.1.1.1 Arguments

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

Table 1
MTS-bind Arguments

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

8.1.1.1.1 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 clause 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**). For secure messaging, when an MS is involved, the **initiator-name** may 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.

8.1.1.1.2 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 ISO/IEC 9594-8).

If only simple-authentication is used, 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**.

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 (eg one or more symmetric-encryption-keys) used to secure the association, or may be absent from the **initiator-bind-token**.

The **initiator-certificate** is a **certificate** of the initiator of the association, generated by a trusted source (eg a certification-authority). It may be supplied by the initiator of the association, if the **initiator-bind-token** is an **asymmetric-token**. 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 compute the **responder-bind-token**. If the responder is known to have, or have access to, the initiator's **certificate** (eg via the Change-credentials abstract-operation, or via the Directory), the **initiator-certificate** may be omitted.

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 clause 8.2.1.4.5) and Delivery-control (see clause 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 ISO/IEC 10021-1).

8.1.1.1.2 Results

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

Table 2
MTS-bind Results

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

8.1.1.1.2.1 Responder-name

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

If the responder is an MTS-user, the name is the **OR-name** of the MTS-user, which is registered with the MTS (see clause 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**). For secure messaging, when an MS is involved, the **responder-name** may 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 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**. 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 (eg one or more symmetric-encryption-keys) used to secure the association, or may be absent from the **responder-bind-token**.

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 ISO/IEC 10021-1).

8.1.1.1.3 Bind-errors

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

8.1.1.2 MTS-unbind

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

8.1.1.2.1 Arguments

The MTS-unbind has no arguments.

8.1.1.2.2 Results

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

8.1.1.2.3 Unbind-errors

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

8.1.2 Bind-errors

This clause defines the following bind-errors:

- a) Authentication-error
- b) Busy
- c) Unacceptable-dialogue-mode
- d) Unacceptable-security-context.

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 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.

8.2 Submission Port

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

8.2.1 Abstract-operations

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

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

8.2.1.1 Message-submission

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

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

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

8.2.1.1.1 Arguments

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

Table 3
Message-submission Arguments (Part 1 of 2)

Argument	Presence	Clause
<i>Originator Argument</i>		
Originator-name	M	8.2.1.1.1.1
<i>Recipient Arguments</i>		
Recipient-name	M	8.2.1.1.1.2
Alternate-recipient-allowed	O	8.2.1.1.1.3
Recipient-reassignment-prohibited	O	8.2.1.1.1.4
Originator-requested-alternate-recipient	O	8.2.1.1.1.5
DL-expansion-prohibited	O	8.2.1.1.1.6
Disclosure-of-recipients	O	8.2.1.1.1.7
<i>Priority Argument</i>		
Priority	O	8.2.1.1.1.8
<i>Conversion Arguments</i>		
Implicit-conversion-prohibited	O	8.2.1.1.1.9
Conversion-with-loss-prohibited	O	8.2.1.1.1.10
Explicit-conversion	O	8.2.1.1.1.11
<i>Delivery Time Arguments</i>		
Deferred-delivery-time	O	8.2.1.1.1.12
Latest-delivery-time	O	8.2.1.1.1.13
<i>Delivery Method Argument</i>		
Requested-delivery-method	O	8.2.1.1.1.14

Table 3
Message-submission Arguments (Part 2 of 2)

Argument	Presence	Clause
<i>Physical Delivery Arguments</i>		
Physical-forwarding-prohibited	O	8.2.1.1.1.15
Physical-forwarding-address-request	O	8.2.1.1.1.16
Physical-delivery-modes	O	8.2.1.1.1.17
Registered-mail-type	O	8.2.1.1.1.18
Recipient-number-for-advice	O	8.2.1.1.1.19
Physical-rendition-attributes	O	8.2.1.1.1.20
Originator-return-address	O	8.2.1.1.1.21
<i>Report Request Arguments</i>		
Originator-report-request	M	8.2.1.1.1.22
Content-return-request	O	8.2.1.1.1.23
Physical-delivery-report-request	O	8.2.1.1.1.24
<i>Security Arguments</i>		
Originator-certificate	O	8.2.1.1.1.25
Message-token	O	8.2.1.1.1.26
Content-confidentiality-algorithm-identifier	O	8.2.1.1.1.27
Content-integrity-check	O	8.2.1.1.1.28
Message-origin-authentication-check	O	8.2.1.1.1.29
Message-security-label	O	8.2.1.1.1.30
Proof-of-submission-request	O	8.2.1.1.1.31
Proof-of-delivery-request	O	8.2.1.1.1.32
<i>Content Arguments</i>		
Original-encoded-information-types	O	8.2.1.1.1.33
Content-type	M	8.2.1.1.1.34
Content-identifier	O	8.2.1.1.1.35
Content-correlator	O	8.2.1.1.1.36
Content	M	8.2.1.1.1.37

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.

The **originator-name** contains the **OR-name** of an individual originator, ie 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 different 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.

8.2.1.1.1.4 Recipient-reassignment-prohibited

This argument indicates whether the message may be reassigned to a **recipient-assigned-alternate-recipient** registered 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 a **recipient-assigned-alternate-recipient**, the message shall be redirected to the **recipient-assigned-alternate-recipient**.

If this argument has the value **recipient-reassignment-prohibited** and the intended-recipient has registered a **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 the **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-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-recipients-allowed** or **disclosure-of-recipients-prohibited**.

In the absence of this argument, the default **disclosure-of-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 clause 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 Recommendation X.408. It may be generated by the originator of the message.

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

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

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

Table 4
Combined Effect of Conversion Arguments

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

8.2.1.1.1.11 Explicit-conversion

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

This argument may have one of the following values: **no-explicit-conversion**, **ia5-text-to-teletex**, **teletex-to-telex**, **telex-to-ia5-text**, **telex-to-teletex**, **telex-to-g4-class-1**, **telex-to-videotex**, **ia5-text-to-telex**, **telex-to-g3-facsimile**, **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-telex**, **videotex-to-ia5-text**, or **videotex-to-teletex**. Other types of **explicit-conversion** may be defined by addenda to this International Standard. **Explicit-conversion** shall be performed as specified in CCITT Recommendation X.408.

In the absence of this argument, the default **no-explicit-conversion** shall be assumed.

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 clause 14.3.2.4.

8.2.1.1.1.14 Requested-delivery-method

This argument indicates the requested 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 (eg using the Directory). If a form of **OR-address** appropriate to a **requested-delivery-method** cannot be found, a **recipient-improperly-specified** abstract-error shall be returned to the originator of the message.

If the **recipient-name** generated by the originator of the message contains an **OR-address** of a form not appropriate to a **requested-delivery-method**, 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 (eg as registered in the Directory in the mhs-preferred-delivery-method attribute), the originator's **requested-delivery-method** takes precedence. If the originator's **requested-delivery-method** conflicts with the originator's conversion requirements (see clauses 8.2.1.1.1.9 to 8.2.1.1.1.11), a non-delivery report shall be returned to the originator of the message.

8.2.1.1.1.15 Physical-forwarding-prohibited

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

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

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

8.2.1.1.1.16 Physical-forwarding-address-request

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

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

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

A physical-forwarding-address may be requested when physical-forwarding is prohibited or allowed (see clause 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 may have one of the following values: **ordinary-mail**, **special-delivery**, **express-mail**, **counter-collection**, **counter-collection-with-telephone-advice**, **counter-collection-with-telex-advice**, **counter-collection-with-teletex-advice**, or **bureau-fax-delivery**.

Note that **bureau-fax-delivery** comprises all A to H modes of delivery defined in CCITT Recommendation F.170, ie: 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** 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: **basic**. Addenda to this International Standard may define other values of this argument. Other values of this argument may be used by bilateral agreement between MDs.

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 shall 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**), ie 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.

Note that 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.

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

Note that in the case of non-delivery-reports delivered to the owner of a DL (see clause 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 the **certificate** of the originator of the message. It shall be generated by a trusted source (eg 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.

The originator's public-asymmetric-encryption-key may be used by the recipient(s) of the message to validate the **message-token**, if an **asymmetric-token** is used.

The originator's public-asymmetric-encryption-key may also be used by the recipient(s) 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 ISO/IEC 10021-1).

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**, rather than the **signed-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**, rather than the **signed-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** instead if confidentiality of the sequence is required.

If the **message-token** is an **asymmetric-token** and the **signed-data** of the **message-token** includes the **content-integrity-check**, the **message-token** provides for non-repudiation-of-origin of the message content (the Non Repudiation of Origin element-of-service, as defined in 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.

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 ISO/IEC 10021-1). It may be generated by the originator of the message.

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

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

If a symmetric-encryption-algorithm is used, the **content-confidentiality-key** used by the originator to encrypt the message content, and which the recipient may use to decrypt the message content, may be

derived from the **message-token** sent with the message. Alternatively, the **content-confidentiality-key** may be distributed by some other means.

If an asymmetric-encryption-algorithm is used, the intended-recipient's public-asymmetric-encryption-key may be used by the originator of the message to encrypt the **message content**. The recipient may use the recipient's secret-asymmetric-encryption-key to decrypt the **message content**. Note that 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(s) 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 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.

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 that 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 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**, and proof of association between the **message-security-label** and the **message content**.

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

The **content-integrity-check** contains the **content-integrity-algorithm-identifier**, and an encrypted function (eg a compressed or hashed version) of the **content-integrity-algorithm-identifier** and the **message content**. Note that the **content-integrity-check** is computed using the clear (ie unencrypted) **message content**.

The content-integrity algorithm may be either a symmetric- or an asymmetric-encryption-algorithm. Note that the use of a symmetric-encryption-algorithm may permit simultaneous compression and encryption of the **message content**.

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.

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** to validate the **content-integrity-check**.

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 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 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 clause 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 (eg by an MTA) without compromising the confidentiality of the message content). Note that if the clear (ie 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 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 to this International Standard may define other forms of **message-origin-authentication-check** (eg based on symmetric-encryption-techniques) which may be used by MTAs through which the message is transferred to authenticate the origin of the message.

8.2.1.1.1.30 Message-security-label

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

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

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

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

If **security-contexts** are established between two MTAs (see clause 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 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 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 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 **unidentified content-type** 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 (see ISO/IEC 10021-6);

interpersonal-messaging-1984: identifies the **interpersonal-messaging-1984** content-type defined in ISO/IEC 10021-7;

interpersonal-messaging-1988: identifies the **interpersonal-messaging-1988** content-type defined in ISO/IEC 10021-7.

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

One specific value of an extended **content-type** which has been defined by this part of ISO/IEC 10021 is:

inner-envelope: an extended **content-type** that is itself a message (envelope and content), for forwarding by the recipient named on the outer-envelope to those named on the inner-envelope. The type of the **content** OCTET STRING is an MTS-APDU encoded using the Basic Encoding Rules of ASN.1. (Note that 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 addenda to this International Standard. Other values of this argument may be used by bilateral agreement between MTS-users.

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 clause 8.2.1.1.1.27).

8.2.1.1.2 Results

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

Table 5
Message-submission Results

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

8.2.1.1.2.1 Message-submission-identifier

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

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

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

8.2.1.1.2.2 Message-submission-time

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

8.2.1.1.2.3 Originating-MTA-certificate

This result contains the **certificate** of the MTA to which the message has been submitted (the originating-MTA). It shall be generated by a trusted source (eg a certification-authority), and may be supplied by the originating-MTA, if the originator of the message requested **proof-of-submission** (see clause 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 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 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 clause 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 (eg a compressed or hashed version) of the **proof-of-submission-algorithm-identifier**, the

arguments of the submitted message (see clause 8.2.1.1.1), and the **message-submission-identifier** and **message-submission-time**. Optional components are included in the **proof-of-submission** if they are present in the message.

Note that 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.

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 8.1.1.1.3 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. Note that if a symmetric-encryption-algorithm is used then the **proof-of-submission** can only support Non Repudiation of Submission if the security-policy in force provides for the involvement of a third party acting as a notary.

8.2.1.1.3 Abstract-errors

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

Table 6
Message-submission Abstract-errors

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

8.2.1.2 Probe-submission

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

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

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

For any **recipient-names** for which redirection would occur, the Probe-submission abstract-operation determines whether the message could be transferred and delivered to the alternate-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 (Part 1 of 2)

Argument	Presence	Clause
<i>Originator Argument</i>		
Originator-name	M	8.2.1.1.1.1
<i>Recipient Arguments</i>		
Recipient-name	M	8.2.1.1.1.2
Alternate-recipient-allowed	O	8.2.1.1.1.3
Recipient-reassignment-prohibited	O	8.2.1.1.1.4
Originator-requested-alternate-recipient	O	8.2.1.1.1.5
DL-expansion-prohibited	O	8.2.1.1.1.6
<i>Conversion Arguments</i>		
Implicit-conversion-prohibited	O	8.2.1.1.1.9
Conversion-with-loss-prohibited	O	8.2.1.1.1.10
Explicit-conversion	O	8.2.1.1.1.11
<i>Delivery Method Argument</i>		
Requested-delivery-method	O	8.2.1.1.1.14
<i>Physical Delivery Argument</i>		
Physical-rendition-attributes	O	8.2.1.1.1.20
<i>Report Request Argument</i>		
Originator-report-request	M	8.2.1.1.1.22

Table 7
Probe-submission Arguments (Part 2 of 2)

Argument	Presence	Clause
<i>Security Arguments</i>		
Originator-certificate	O	8.2.1.1.1.25
Probe-origin-authentication-check	O	8.2.1.2.1.1
Message-security-label	O	8.2.1.1.1.30
<i>Content Arguments</i>		
Original-encoded-information-types	O	8.2.1.1.1.33
Content-type	M	8.2.1.1.1.34
Content-identifier	O	8.2.1.1.1.35
Content-correlator	O	8.2.1.1.1.36
Content-length	O	8.2.1.2.1.2

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 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 to this International Standard may define other forms of **probe-origin-authentication-check** (eg based on symmetric-encryption-techniques) which may be used by MTAs through which the probe is transferred to authenticate the origin of the probe.

8.2.1.2.1.2 Content-length

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

8.2.1.2.2 Results

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

Table 8
Probe-submission Results

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

8.2.1.2.2.1 Probe-submission-identifier

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

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

8.2.1.2.2.2 Probe-submission-time

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

8.2.1.2.3 Abstract-errors

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

Table 9
Probe-submission Abstract-errors

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

8.2.1.3 Cancel-deferred-delivery

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

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

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

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

8.2.1.3.1 Arguments

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

Table 10
Cancel-deferred-delivery Arguments

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

8.2.1.3.1.1 Message-submission-identifier

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

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

8.2.1.3.2 Results

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

8.2.1.3.3 Abstract-errors

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

Table 11
Cancel-deferred-delivery Abstract-errors

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

8.2.1.4 Submission-control

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

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

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

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

8.2.1.4.1 Arguments

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

Table 12
Submission-control Arguments

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

8.2.1.4.1.1 Restrict

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

This argument may have one of the following values:

update: the other arguments update the prevailing controls;

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

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

8.2.1.4.1.2 Permissible-operations

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

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

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

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

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

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

8.2.1.4.1.3 Permissible-lowest-priority

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

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

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

8.2.1.4.1.4 Permissible-maximum-content-length

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

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

8.2.1.4.1.5 Permissible-security-context

This argument temporarily limits the sensitivity of submission-port abstract-operations (submission-security-context) that the MTS-user may invoke on the MTS. It is a temporary restriction of the **security-context** established when the association was initiated (see clause 8.1.1.1.3). It may be generated by the MTS.

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

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

8.2.1.4.2 Results

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

Table 13
Submission-control Results

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

8.2.1.4.2.1 Waiting-operations

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

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

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

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

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

8.2.1.4.2.2 Waiting-messages

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

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

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

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

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

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

8.2.1.4.2.3 Waiting-encoded-information-types

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

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

8.2.1.4.2.4 **Waiting-content-types**

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

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

8.2.1.4.3 **Abstract-errors**

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

Table 14
Submission-control Abstract-errors

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

8.2.2 **Abstract-errors**

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

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

8.2.2.1 **Submission-control-violated**

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

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

8.2.2.2 Element-of-service-not-subscribed

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

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

8.2.2.3 Deferred-delivery-cancellation-rejected

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

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

8.2.2.4 Originator-invalid

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

The Originator-invalid abstract-error has no parameters.

8.2.2.5 Recipient-improperly-specified

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

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

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

8.2.2.6 Message-submission-identifier-invalid

The Message-submission-identifier-invalid abstract-error reports that the deferred-delivery of a message cannot be cancelled because the specified **message-submission-identifier** is invalid.

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

8.2.2.7 Inconsistent-request

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

The Inconsistent-request abstract-error has no parameters.

8.2.2.8 Security-error

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

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

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

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 clause 9.1) but is unsupported by the MTS.

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

8.2.2.10 Remote-bind-error

The Remote-bind-error abstract-error reports that the requested abstract-operation cannot be provided by the MS because the MS is unable to bind to the MTS. Note that this abstract-error only occurs on an indirect submission to the MTS 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 (Part 1 of 2)

Argument	Presence	Clause
<i>Delivery Arguments</i>		
Message-delivery-identifier	M	8.3.1.1.1.1
Message-delivery-time	M	8.3.1.1.1.2
Message-submission-time	M	8.2.1.1.2.2
<i>Originator Argument</i>		
Originator-name	M	8.2.1.1.1.1
<i>Recipient Arguments</i>		
This-recipient-name	M	8.3.1.1.1.3
Intended-recipient-name	C	8.3.1.1.1.4
Redirection-reason	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
<i>Priority Argument</i>		
Priority	C	8.2.1.1.1.8
<i>Conversion Arguments</i>		
Implicit-conversion-prohibited	C	8.2.1.1.1.9
Conversion-with-loss-prohibited	C	8.2.1.1.1.10
Converted-encoded-information-types	C	8.3.1.1.1.8
<i>Delivery Method Argument</i>		
Requested-delivery-method	C	8.2.1.1.1.14
<i>Physical Delivery Arguments</i>		
Physical-forwarding-prohibited	C	8.2.1.1.1.15
Physical-forwarding-address-request	C	8.2.1.1.1.16
Physical-delivery-modes	C	8.2.1.1.1.17
Registered-mail-type	C	8.2.1.1.1.18
Recipient-number-for-advice	C	8.2.1.1.1.19
Physical-rendition-attributes	C	8.2.1.1.1.20
Originator-return-address	C	8.2.1.1.1.21
Physical-delivery-report-request	C	8.2.1.1.1.24