Stable Implementation Agreements for Open Systems Interconnection Protocols: Part 8 - 1988 Message Handling Systems

Output from the June 1991 NIST Workshop for Implementors of OSI

SIG Chair: **Barbara Nelson (Retix)**
SIG Editor: **Rich Ankney (Simpact)**

Foreword

This part of the Stable Implementation Agreements was prepared by the Message Handling Systems Special Interest Group (X.400 SIG) of the National Institute of Standards and Technology (NIST) Workshop for Implementors of Open Systems Interconnection (OIW).

Text in this part has been approved by the Plenaries of the X.400 SIG and of the OIW. This part replaces the previously existing chapter on this subject. Additional material has been included recently. Annexes C, D, E, and F are for information only.

Future changes and additions to this version of these Implementor Agreements will be published as change pages. Deleted and replaced text will be shown as strikeout. New and replacement text will be shown as shaded.

Table of Contents

Annex D (informative)

Annex E (informative)

List of Figures

List of Tables

Part 8 1988 Message Handling Systems

0 Introduction

This is an Implementation Agreement developed by the Implementor's Workshop sponsored by the U. S. National Institute of Standards and Technology to promote the useful exchange of data between devices manufactured by different vendors. This Agreement is based on, and employs protocols developed in accord with, the OSI Reference Model. It provides detailed guidance for the implementor and eliminates ambiguities in interpretations.

This is an Implementation Agreement for Message Handling Systems (MHS) based on both the CCITT X.400 (1988) series of Recommendations and the similar (but not identical) ISO MOTIS standard (see References). These Recommendations and Standards are referred to as the *base standards*. The term 'MHS' is used to refer to both sources where a distinction is unnecessary. Similarly, '1984' and '1988' are often used to distinguish between the CCITT X.400 (1984) series of Recommendations and the later sources.

This Implementation Agreement seeks to establish a common specification which is conformant with both CCITT and ISO with a view to:

a) Preventing a proliferation of incompatible communities of MHS systems which are isolated for protocol reasons;

b) Achieving interworking with implementations conforming to the OIW Stable Implementation Agreements for CCITT 1984 X.400-based Message Handling Systems;

c) Facilitating integration of other OSI-based services (e.g., Directory) within a single real system.

This initial Implementation Agreement is designed to encourage early upgrade of existing 1984-based systems as follows:

a) To add 1988 functionality (Message Store, Remote User Agent, etc);

b) To provide additional functionality above the minimal conformant 1988 MHS defined in the December 1989 version of the OIW Implementation Agreements. Subsequent versions of this Agreement will define such additional 1988 aspects as incremental enhancements.

However, it is considered that the OIW Stable Implementation Agreements for CCITT 1984 X.400-based Message Handling Systems (Part 7) should not be withdrawn at this stage. It is anticipated that X.400 (1984) implementations will continue to provide a viable alternative for applications that do **not** require the additional 1988 functionality for some time.

1 Scope

This Agreement specifies the requirements for MHS implementations based on the 1988 MHS standards.

This Agreement applies equally to Private Management Domains (PRMDs) and Administration Management Domains (ADMDs). Four boundary interfaces are specified, as illustrated in figure 1:

a) Management Domain (MD) to MD;

b) Message Transfer Agent (MTA) to MTA within a domain;

c) MTA to remote Message Store (MS) or User Agent (UA);

d) MS to Remote UA.

MHS protocols other than the Message Transfer Protocol (P1), the Message Transfer System Access Protocol (P3), the Interpersonal Messaging Protocol (P2), and the Message Store Access Protocol (P7) are beyond the scope of this Agreement. Issues arising from the use of other protocols are outside the scope of this document. This Agreement describes the services provided at each interface shown in figure 1.

MHS implementations may be configured as any single or multiple occurrence or combination of MTA, MS and UA, as illustrated in figure 1. It is not intended to restrict the types of system that may be configured for conformance to this Agreement (although it is equally recognized that not all configuration types may be commercially viable).

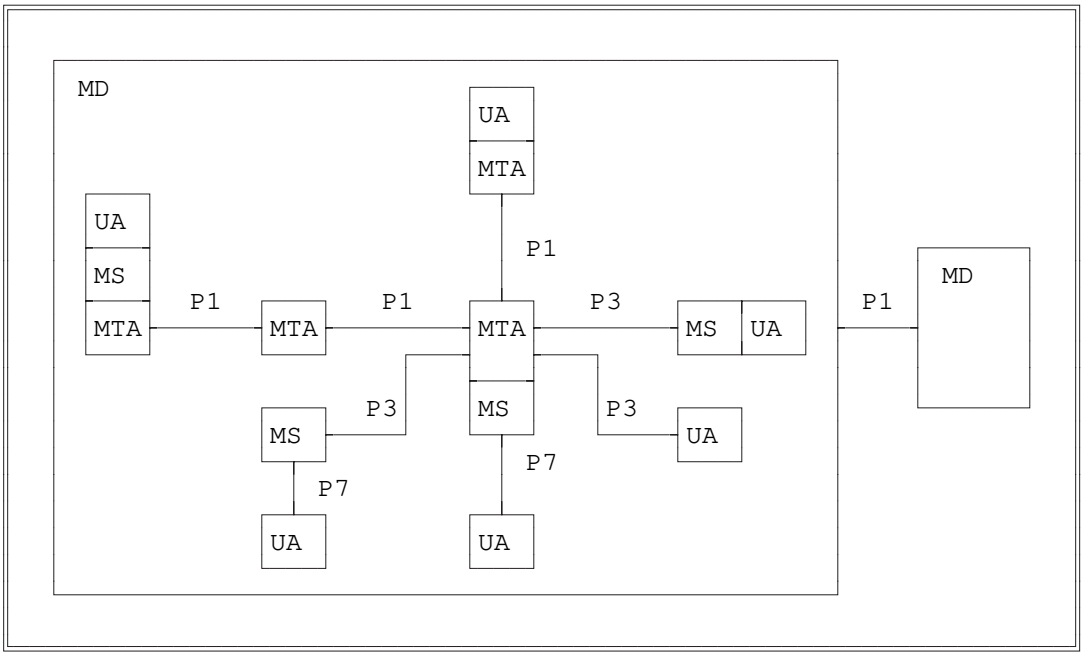

Figure 1 - Scenario Definition.

The 1988 MHS standards cover a wide and diverse range of functional areas, not all of which would be

relevant to every implementation. In order to achieve a more precise definition of conformance requirements according to the functionality supported by an implementation, and additionally to facilitate future enhancement of this initial specification, the concept of *Functional Groups* has been introduced. Conformance requirements for support of Functional Groups by particular configurations are specified in clause 16.

In the context of these agreements, the term "Support" means that the service provider makes the element of service (and related elements of protocol) available to the service user. The service user provides adequate access to invoke the elements of service and/or makes information associated with the service element available. Additionally, for "Not Defined" or "Not Applicable" elements, the service provider is not required to make the element available to the service user. However, the service provider should not regard the occurrence of the corresponding protocol elements as an error and should relay those elements. Naturally, protocol elements marked critical for submission, transfer, or delivery must be processed according to the base standards.

The following functional groups are covered by this Implementors Agreement:

a) The MT Kernel in clause 5;

b) The IPM Kernel in clause 6;

c) The Message Store in clause 7;

d) Remote User Agent support in clause 8;

e) Distribution Lists in 9.2 (which are for further study);

f) Use of Directory in 9.3;

g) MHS Management in clause 10 (which is for further study);

h) Security in clause 11;

i) The Physical Delivery Access Unit in 12.1 (which is for further study);

j) Other Access Units in 12.2 (which are for further study);

k) Conversion in clause 13 (which is for further study);

l) Redirection in clause 14 (which is for further study);

m) The EDI Messaging Service in clause 15 (which is for further study).

2 Normative References

2.1 CCITT

Application Layer - MHS

CCITT Recommendation X.400 (1988), *Message Handling, System and Service Overview*.

CCITT Recommendation X.402 (1988), *Message Handling Systems, Overall Architecture*.

CCITT Recommendation X.407 (1988), *Message Handling Systems, Abstract Service Definition Conventions*.

CCITT Recommendation X.411 (1988), *Message Handling Systems, Message Transfer System: Abstract Service Definition and Procedures*.

CCITT Recommendation X.413 (1988), *Message Handling Systems, Message Store: Abstract Service Definition*.

CCITT Recommendation X.419 (1988), *Message Handling Systems, Protocol Specifications*.

CCITT Recommendation X.420 (1988), *Message Handling Systems, Interpersonal Messaging System*.

CCITT Recommendation X.121 (1988), *International Numbering Plan*.

CCITT draft Recommendation X.435 (June 1990), *Message Handling Systems, EDI Messaging System, Protocol Specifications*.

CCITT draft Recommendation F.435 (June 1990), *Message Handling Systems, EDI Messaging System, Abstract Service Definition*.

2.2 ISO

Application Layer - MHS

ISO 10021-1 *Information Processing Systems - Text Communication - MOTIS - System and Service Overview*.

ISO 10021-2 *Information Processing Systems - Text Communication - MOTIS - Overall Architecture*.

ISO 10021-3 *Information Processing Systems - Text Communication - MOTIS - Abstract Service Definition Conventions*.

ISO 10021-4 *Information Processing Systems - Text Communication - MOTIS - Message Transfer System: Abstract Service Definition and Procedures*.

ISO 10021-5 *Information Processing Systems - Text Communication - MOTIS - Message Store: Abstract Service Definition*.

ISO 10021-6 *Information Processing Systems - Text Communication - MOTIS - Protocol Specifications*.

ISO 10021-7 *Information Processing Systems - Text Communication - MOTIS - Interpersonal Messaging System*.

3 Status

This version of the *Implementation Agreements for Message Handling Systems (MHS)* is under development. It is based on the CCITT X.400 (1988) Recommendations and ISO MOTIS (10021, parts 1-7) standards, as amended by the *MHS Implementors Guide*, version 3.

It is intended that the Stable Implementation Agreements will initially include an Agreement which specifies a minimal 1988-based MHS implementation and support for Message Stores and Remote User Agents, and which addresses interworking with 1984-based implementations. The remaining features specified in the 1988 standards will be covered in subsequent versions of this Agreement.

This initial version has not yet been aligned with other MHS profiles, so changes may be necessary in the future for international harmonization, (e.g., support for international character repertoires and conversion).

4 Errata

No Errata to Stable material at this time.

5 MT Kernel

5.1 Introduction

This clause specifies the requirements for a minimal 1988-based MTS implementation (i.e., MTA) which is capable of interworking with 1984-based MTAs. The 'base' MT Service specified in this clause does **not** include:

a) Message Store (see clause 7);

b) Remote UA (see clause 8);

c) Use of Directory Services (see 9.3);

d) Distribution Lists (see 9.2);

e) Security (see clause 11);

f) Interworking with Physical Delivery systems or Specialized Access (see clause 12);

g) Conversion (see clause 13).

Such a minimal 1988-based MTA will have the following capabilities in order to achieve interworking with 1984-based MTAs and to facilitate migration to full 1988 operation:

a) It will be protocol-conformant to 1988 P1;

b) It will downgrade 1988 P1 to 1984 P1 when relaying to 1984-based MTAs, as specified in Annex B of X.419 (see clause 5.5);

c) It will support both 'normal' mode and 'X.410-1984' ('passthrough') mode protocol stacks (i.e., as required by ISO and CCITT respectively);

d) A conforming implementation shall obey the criticality mechanism defined in the base standards. The following abstract operations are made critical for delivery for these Implementation Agreements: message token, content integrity check, and content confidentiality algorithm Id.

5.2 Elements of Service

This clause specifies the requirements for support of MT Elements of Service by an MTA conforming to the MT Kernel Functional Group of this Agreement.

The classification scheme for support of Elements of Service is as follows:

Mandatory (M): the Element of Service must be supported and made available to the service user;

Optional (O): the Element of Service may be supported, but is not required for conformance to this Agreement;

Out of Scope (I): the Element of Service is outside the scope of these Implementation Agreements;

Not Applicable (-): the Element of Service is not applicable in the particular context according to the base standard;

To Be Determined (*): the support classification for the Element of Service has yet to be determined.

The requirements for support of MT Elements of Service for origination and reception and (where relevant) relaying are distinguished. Elements of Service which are new in the 1988 MHS standards are indicated as (1988).

An MTA must support those Basic MT Elements of Service and MT Optional User Facilities defined in section 19 of X.400 (1988) as listed and qualified in tables 1 and 2.

Specification of dynamic behavior in these agreements will only be included in those cases where there is an identified functional objective which is not satisfied by the specification of dynamic behavior in the

corresponding base standard(s) and where the resulting behavior does not breach base standard conformance requirements.

In these exceptional cases, there may be situations where these agreements must specify the dynamic behavior of an implementation as distinguished in annex C of ISO TR-10 000. Where this occurs, a table of dynamic conformance requirements will be presented using the classification scheme below:

Mandatory (M): The element must be implemented although use is not required for conformance to the base standard. The element shall always be used for conformance to these agreements.

Excluded (X): This element must either not be implemented, or it must be possible to prevent use of the element.

NOTE - As stated in 6.7 of ISO TR-10 000-1, restrictions by a profile on the dynamic conformance requirements of a base standard are exceptions, and should only apply to transmission. Restrictions should not apply to reception. In the case of Excluded options, it must be possible to ensure that such options are not initiated or transmitted. However, it is still possible that an implementation may receive an Excluded element from an implementation which does not conform to the same profile.

Table 1 - MT Kernel: Basic MT Elements of Service

Element of Service	Origination	Reception	Relaying
Access Management	M[1]	M[1]	–
Content Type Indication	M	M	–
Converted Indication	M	M	M
Delivery Time Stamp Indication	–	M	–
Message Identification	M	M	–
Non-delivery Notification	M	M	M
Original Encoded Information Types Indication	M	M	–
Submission Time Stamp Indication	M	M	–
User/UA Capabilities Registration (1988)	–	M[1]	–

Notes
1 A local matter in the case of collocated UA/MTA and/or MS/MTA configurations.

Table 2 - MT Kernel: MT Service Optional User Facilities

Element of Service	Origination	Reception	Relaying
Alternate Recipient Allowed	M	M[2]	–
Alternate Recipient Assignment	–	O[2]	–
Conversion Prohibition	M	M	M
Conversion Prohibition in Case of Loss of Information (1988)	O	O	O
Deferred Delivery	M[3]	O	O
Deferred Delivery Cancellation	M[6]	–	–
Delivery Notification	M	M	–
Disclosure of Other Recipients	M	M	M
DL Expansion History Indication	–	M[4]	–
DL Expansion Prohibited	M[5]	–	–
Explicit Conversion	O	O	O
Grade of Delivery Selection	M	M	M
Hold for Delivery	–	M[1]	–
Implicit Conversion	O	O	O
Latest Delivery Designation (1988	O	O	O
Multi Destination Delivery	M	M	M
Originator Requested Alternate Recipient (1988)	O	O	–
Prevention of Non-delivery Notification	M	–	–
Probe	M	M	M
Redirection Disallowed by Originator (1988)	M	M	–
Redirection of Incoming Messages (1988)	–	O	–
Requested Delivery Method (1988)	M	M	–
Restricted Delivery (1988)	–	O	–
Return of Content	O	O	O

Notes

1 A local matter in the case of collocated UA/MTA and/or MS/MTA configurations.

2 If Alternate Recipient Assignment is supported on reception, then support of Alternate Recipient Allowed is Mandatory on reception; otherwise, support of Alternate Recipient Allowed is not applicable on reception.

3 Support of this MT Element of Service is Mandatory for conformance reasons, but may be performed as a local matter to the originating MTA.

4 Support of this MT Element of Service refers only to the delivery of DL expansion history and not to the performing of DL expansion (see clause 9.2).

5 Support of this MT Element of Service does not imply the capability to perform DL expansion (see clause 9.2).

6 Messages should be held in the originating MTA to provide support for this element of service.

5.3 MTS Transfer Protocol (P1)

The requirements for support of MTS Transfer Protocol (P1) elements are detailed in clause 1 of annex A.

Support of MTS Transfer Protocol application contexts by an MTA is classified as in table 3.

Table 3 - Application Contexts Classification

Application Context	Support
mts-transfer-protocol-1984	Mandatory
mts-transfer-protocol	Mandatory
mts-transfer	Mandatory

Use of the underlying services to support these application contexts is specified in clause 14.

5.4 MTS - APDU Size

See Working Document.

5.5 1988/84 Interworking Considerations

See Working Document.

6 IPM Kernel

6.1 Introduction

This clause specifies the requirements for a minimal 1988-based IPMS implementation (i.e., UA) which is capable of interworking with 1984-based UAs. The 'base' IPM Service specified in this clause does **not** include:

a) Message Store (see clause 7);

b) Remote UA (see clause 8);

c) Use of Directory Services (see 9.3);

d) Distribution Lists (see 9.2);

e) Security (see clause 11);

f) Interworking with Physical Delivery systems or Specialized Access (see clause 12).

Such a minimal 1988-based UA will have the following capabilities in order to achieve interworking with 1984-based UAs and to facilitate migration to full 1988 operation:

a) It will continue to support content type P2 (encoded as integer 2) on origination and reception;

b) It will support receipt of P2 (encoded as integer 22);

c) It may originate P2 encoded as integer 22, but the guidelines specified in section 8.18.2 of X.420 (1988) are to be followed, i.e. the content type shall be encoded as integer 2 unless 1988 P2 protocol elements are present. All IPM UAs must support either MTS Submission and Delivery based on the protocol classifications in clause 3 of annex A, or MS Submission and Retrieval based on the protocol classifications in clause 4 of annex A. However, how such information is conveyed to/from the MTS or MS in the case of a collocated UA is a local matter, and will not necessarily be subject to conformance verification.

6.2 Elements of Service

This clause specifies the requirements for support of IPM Elements of Service by a UA conforming to the IPM Kernel Functional Group of this Agreement.

The classification scheme for support of Elements of Service is as defined in 5.2.

The requirements for support of IPM Elements of Service for origination and reception are distinguished. Elements of Service which are new in the 1988 MHS standards are indicated as (1988).

A UA must support those Basic IPM Elements of Service and IPM Optional User Facilities defined in section 19 of X.400 (1988) as listed and qualified in tables 4 and 5.

Table 4 - IPM Kernel: Basic IPM Elements of Service

Element of Service	Orig	Recep
Access Management	M[1]	M[1]
Content Type Indication	M	M
Converted Indication	-	M
Delivery Time Stamp Indication	-	M
IP-message Identification	M	M
Message Identification	-	M
Non-delivery Notification	M	-
Original Encoded Information Types Indication	M	M
Submission Time Stamp Indication	M	M
Typed Body	M	M
User/UA Capabilities Registration (1988)	-	M[1]

Notes
1 In the case of a collocated UA/MTA or collocated UA/MS, the method and extent to which this Element of Service is provided is a local matter; it is not necessarily testable in the absence of support for the P3 or P7 protocol.

Table 5 - IPM Kernel: IPM Service Optional User Facilities

Element of Service	Orig	Recep
Alternate Recipient Allowed	O	–
Alternate Recipient Assignment	–	O
Authorizing Users Indication	O	M
Auto-forwarded Indication	O	M
Blind Copy Recipient Indication	O	M
Body Part Encryption Indication	O	M
Conversion Prohibition	M	M
Conversion Prohibition in Case of Loss of Information (1988)	O	O
Cross Referencing Indication	O	M
Deferred Delivery	M	–
Deferred Delivery Cancellation	O	–
Delivery Notification	M	–
Disclosure of Other Recipients	O	M
DL Expansion History Indication (1988)	–	M
DL Expansion Prohibited (1988)	M	–
Expiry Date Indication	O	M
Explicit Conversion	O	–
Forwarded IP-message Indication	O	M
Grade of Delivery Selection	M	M
Hold for Delivery	–	O
Implicit Conversion	–	O
Importance Indication	O	M
Incomplete Copy Indication (1988)	O	O
Language Indication (1988)	O	M
Latest Delivery Designation (1988)	O	–
Multi-Destination Delivery	M	–
Multi-part Body	O	M
Non-receipt Notification Request	O	M[1]
Obsoleting Indication	O	M
Originator Indication	M	M
Originator Requested Alternate Recipient (1988)	O	–
Prevention of Non-delivery Notification	O	–
Primary and Copy Recipients Indication	M	M
Probe	O	–
Receipt Notification Request Indication	O	O
Redirection Disallowed by Originator (1988)	O	–
Redirection of Incoming Messages (1988)	–	O
Reply Request Indication	O	M
Replying IP-message Indication	M	M
Requested Delivery Method (1988)	M	–

Table 5 - IPM Kernel: IPM Service Optional User Facilities (concluded)

Element of Service	Orig	Recep
Restricted Delivery (1988)	–	O
Return of Content	O	–
Sensitivity Indication	O	M
Subject Indication	M	M
Use of Distribution List (1988)	O	–

Notes
1 Support of Non-Receipt Notification Request on reception does not require the capability to generate a non-receipt notification in the case of an implementation in which a non-receipt condition cannot occur.

6.3 Interpersonal Messaging Protocol (P2)

The requirements for support of Interpersonal Messaging Protocol (P2) elements are detailed in clause 2 of annex A.

6.4 Body Part Support

This clause specifies the requirements for support of IPM body part types by a UA conforming to this Agreement.

The classification scheme for support of IPM body part types is as defined in 5.2.

The requirements for support of IPM body part types for origination and reception are distinguished. Body part types which are new in the 1988 MHS standards are indicated as (1988).

A UA must support those IPM body part types defined in Annex E of X.420 (1988) as listed and qualified in table 6. If an implementation supports a particular body part type for reception, it should also be able to support that body part type for reception if it is part of a forwarded message.

Any basic body part type that is supported on reception must be supported as integer encoding (ASN.1 context-specific identifier) and as object identifier (externally-defined) encoding.

All body parts with integer-encoded identifiers in the range 0 up to and including 16K-1 are legal. Body part integer-encoded identifiers corresponding to X.121 country codes should be interpreted as described in figure 4. These privately-defined body part types are specified as an interim measure to provide backward compatibility with 1984 MHS implementations. For interworking between UAs based on the 1988 (or later) MHS standards, it is strongly recommended that the externally-defined body part be used instead.

Table 6 - IPM Kernel: Body Part Types

Body Part Type		Orig	Recep
IA5Text		M	M
Voice		O	O
G3Facsimile		O	O
G4Class1	(TIF0)	O	O
Teletex		O	O
Videotex		O	O
Encrypted		O	O
Message	(ForwardedIPMessage)	O	M
MixedMode	(TIF1)	O	O
BilaterallyDefined	(Unidentified)	O	O
NationallyDefined		O	O
ExternallyDefined	(1988)	O	O/M[1]
PrivatelyDefined	(see figure 4)	O	O
GeneralText	(1988 - extended)	*	*

Notes

1 Any basic body part type that is supported on reception as integer encoding must also be supported as object identifier encoding. Support for all other externally defined body parts is optional.

```
BodyPart              ::=  CHOICE {
  ia5-text                   [0] IA5TextBodyPart,
                             .
  externally-defined         [15] ExternallyDefinedBodyPart,
                             .
                             [234] UKBodyParts,
                             .
                             [310] USABodyParts,
                             .        }

Where UKBodyParts and USABodyParts (privately defined) are
defined as:

                             SEQUENCE {BodyPartNumber, ANY}

BodyPartNumber        ::=  INTEGER

These privately-defined body part types are specified as an
interim measure to provide backward compatibility with 1984
MHS implementations.  For interworking between UAs based on
the 1988 (or later) MHS standards, it is strongly
recommended that the externally-defined body part be used
instead.

The undefined bit in P1 EncodedInformationTypes must be set
when a message contains a privately defined body part. Each
UA that expects such body parts should include undefined in
the set of deliverable EncodedInformationTypes it registers
with the MTA.

Body part numbers are interpreted relative to the body part
type in which they are used.  OIW registers body part
numbers for privately-defined formats within the United
States.
```

Figure 4 - Privately-Defined Body Parts.

7 Message Store

7.1 Introduction

This clause specifies Agreements for implementation of the Message Store (MS) Functional Group. The MS is responsible for accepting delivery of messages on behalf of a single end-user, and retaining the messages until the end-user's UA is able to retrieve them. Message submission and some administration services are provided via "pass-through" to the MTS. Figure 5 illustrates the logical relationship of the MS to the UA and MTS.

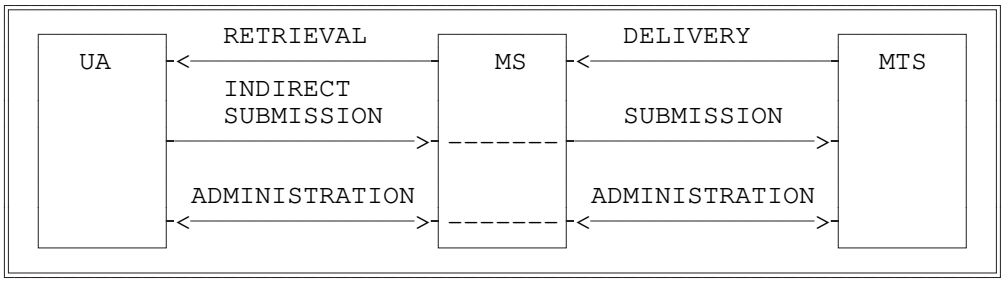

Figure 5 - Message Store Model.

The Agreements in this clause specify the Message Store's use of the retrieval, delivery, and administration services. Agreements on submission services are specified in clause 8, which describes support for the Remote UA.

The goal of the Agreements in this clause is to define the minimal set of features which are necessary to provide useful Message Store services, independent of the MTA implementation version (i.e., 1984 or 1988).

7.2 Scope

The scope of the Agreements in this clause is depicted in figure 6, and is confined to the services and protocols between the boundaries shown (marked with asterisks). Requirements for the UA and MTA are addressed only to the extent that they affect the Message Store and Remote User Agent services and protocols. This reflects the additional services required at the UA to support MS access and at the MTA to support a remote MS.

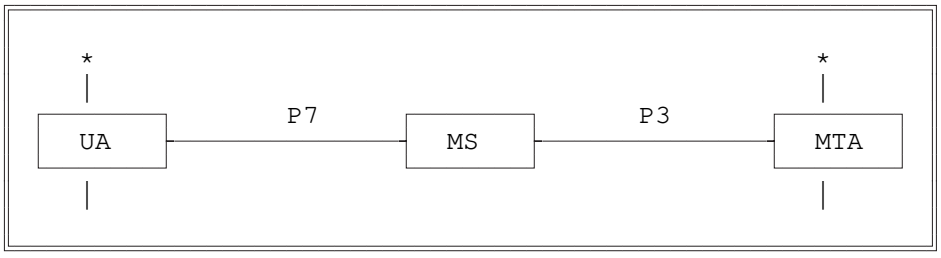

Figure 6 - Scope of Message Store Agreements.

The UA, MS and MTA configuration is not restricted; any of these components may be collocated, although they are depicted as logically separate. In the case of a collocated UA and MS, a proprietary interface may be used instead of P7. In the case of a collocated MS and MTA, a proprietary interface may be used instead of P3.

7.3 Elements of Service

This clause specifies the requirements for support of Elements of Service to provide a Message Store conforming to the Message Store Functional Group of this Agreement.

The classification scheme for support of Elements of Service is as defined in clause 5.2.

Support for Elements of Service is specified in table 7 both for the Message Store itself and for the User Agent.

Table 7 - Message Store: Elements of Service

Element of Service	UA	MS
Stored Message Deletion	M	M
Stored Message Fetching	M	M
Stored Message Listing	M	M
Stored Message Summary	M	M
Stored Message Alert	O	O
Stored Message Auto Forward	O	O

7.4 Attribute Types

Requirements for support of the attributes used in the Message Store are detailed in clauses 8 and 10 of annex A. Clause 8 of annex A specifies support for the General Attributes of the Message Store, while clause 10 of annex A specifies support for the IPM Message Store Attributes.

There are three classes of support for General Attributes in the Message Store: Basic, IPM, and EDIMG.

The Basic MS is intended to support the use of the MS as a continuously available, reliable device (such as a spooling entity) for receiving, storing, and forwarding messages and reports. The Basic MS is not required to support any IPM or EDIMG attributes.

The IPM MS provides more flexible access to the General Attributes as well as supporting IPM Attributes.

IPM User Agents can make use of either the Basic or IPM MS.

Clause A.10 of annex A is to be read in accordance with annex C of X.420 (1988).

EDI UA can make use of either Basic or EDI MS. Clause A.12 of annex A is to be read in accordance with annex C of X.435.

7.5 Pragmatic Constraints for Attribute Types

There are no additional pragmatic constraints for attribute types beyond those of the base standards.

7.6 Implementation of the MS with 1984 Systems

While the Message Store is part of the 1988 MHS standards, implementation of MS services with a 1984 MTA is possible. In order to interoperate with other 1984 MHS systems, implementations with this configuration should adhere to the following guidelines:

a) The UA must generate 1984 P2 PDUs;

b) The UA must identify the content protocol as integer 2 to the MS;

c) The MS must be collocated with the MTA unless 1988 P3 support is provided on the 1984 MTA as well.

To meet these guidelines, the UA may be implemented as follows:

a) The UA could conform to X.420 (1984), with 1988 UA extensions for utilizing the MS services;

b) The UA could be a 1988 UA with restrictions on protocol elements generated and by identifying the content type as integer 2 rather than 22. No 1988-specific elements should be generated.

Details of the interface between the 1988 MS and the 1984 MTA when collocated are beyond the scope of these Agreements.

7.7 MS Access Protocol (P7)

The requirements for support of MS Access Protocol (P7) elements by an MS and a remote MS-user are detailed in clause 4 of annex A.

The requirements for support of MS Access Protocol (P7) application contexts by an MS and an MS-user are as specified in clauses 6.1 and 10.1 of X.419 (1988) (ISO 10021-6) with the **additional** requirement that an MS-user **must** at least support the ms-access application context, as defined in table 8.

Table 8 - Application Contexts Support for P7

Application Context	MS	MS-user
ms-access	Mandatory	Mandatory
ms-reliable-access	Optional	Optional

Use of the underlying services to support these application contexts is specified in clause 14.

7.8 MTS Access Protocol (P3)

The requirements for support of MTS Access Protocol (P3) elements by an MTA and an MS where the MS is **not** collocated with the MTA are detailed in clause A.3 of annex A.

The requirements for support of MTS Access Protocol (P3) application contexts by an MTA and an MS in such a scenario are as specified in sections 6.1 and 10.1 of X.419 (1988) (ISO 10021-6) with the **additional** requirement that a remote MS **must** at least support the mts-access and mts-forced-access application contexts, as defined in table 9.

Table 9 - Application Contexts Support for P3

Application Context	MTA	MS
mts-access	Mandatory	Mandatory
mts-forced-access	Mandatory	Mandatory
mts-reliable-access	Optional	Optional
mts-forced-reliable-access	Optional	Optional

Use of the underlying services to support these application contexts is specified in clause 14.

8 Remote User Agent Support

8.1 Introduction

This clause specifies Agreements for implementation of the Remote User Agent Functional Group, i.e. for support of an IPM UA that is **not** collocated with its MTA.

NOTE - Support of other classes of UA is for further study.

The goal of the Agreements in this clause is to define the minimal set of features which are necessary to provide useful Remote User Agent services, independent of the MTA implementation version (i.e., 1984 or 1988).

8.2 Scope

The scope of the Agreements in this clause is depicted in figure 7, and is confined to the services and protocols between the boundaries shown (marked with asterisks). Requirements for the UA and MTA are addressed only to the extent that they affect the Remote User Agent services and protocols. Access to a Message Store by a Remote User Agent is covered in clause 7.

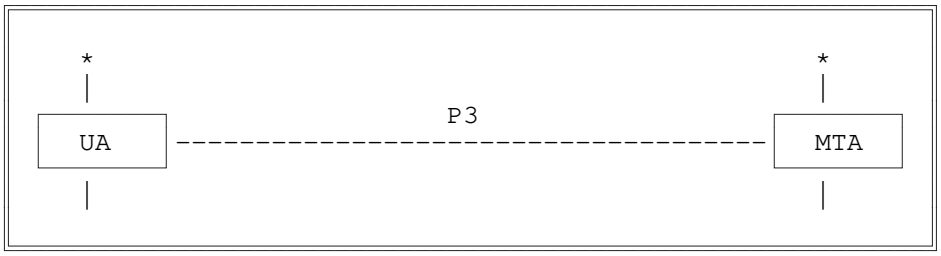

Figure 7 - Scope of Remote User Agent Agreements

8.3 Elements of Service

This clause specifies the requirements for support of Elements of Service for conformance to the Remote User Agent Functional Group of this Agreement.

The classification scheme for support of Elements of Service is as defined in 5.2.

Support for Elements of Service is specified both for the MT Service (table 10) and for the IPM Service (table 11), and is in addition to the support requirements specified in clauses 5 and 6 if this Functional Group is supported.

Table 10 - Remote User Agent Support: MT Elements of Service

Element of Service	Origination	Reception
Access Management	M	M
Hold for Delivery	-	M
User/UA Capabilities Registration	-	M

Table 11 - Remote User Agent Support: IPM Elements of Service

Element of Service	Origination	Reception
Access Management	M	M
Hold for Delivery	-	M
User/UA Capabilities Registration	-	M

8.4 MTS Access Protocol (P3)

The requirements for support of MTS Access Protocol (P3) elements by an MTA and an MTS-user (whether UA or UA/MS) where the MTS-user is **not** collocated with the MTA are detailed in clause A.3 of annex A.

The requirements for support of MTS Access Protocol (P3) application contexts by an MTA and an MTS-user in such a scenario are as specified in sections 6.1 and 10.1 of X.419 (1988) (ISO 10021-6) with the **additional** requirement that a remote MTS-user **must** at least support the mts-access and mts-forced-access application contexts, as defined in table 12.

Table 12 - Application Contexts Support for P3

Application Context	MTA	MTS-user
mts-access	Mandatory	Mandatory
mts-forced-access	Mandatory	Mandatory
mts-reliable-access	Optional	Optional
mts-forced-reliable-access	Optional	Optional

Use of the underlying services to support these application contexts is specified in clause 14.

9 Naming, Addressing & Routing

9.1 Use of O/R Addresses for Routing

Procurers are responsible for understanding the implications of routing requirements and capabilities.

9.2 ORAddress Attribute List Equivalence Rules

Two ORAddresses are equivalent if each contains the same set of attributes and each attribute compares in type and value.

The following equivalence rules apply when comparing a provided ORAddress with a collection of known ORAddresses. For example, in order to perform delivery of a message to a recipient, the MTA must unambiguously match the ORAddress contained in the message with the known ORAddresses. See X.402 (1988), section 18.4, for the base standard attribute equivalence rules. The following additional rules must also be applied by the delivering (or non-delivering) MTA:

a) If the provided ORAddress is an unambiguous underspecification of a known ORAddress, the ORAddresses are equivalent. For example, if the initials were omitted, the ORAddress would still be equivalent. Under-specification means that some attributes that are not present in the provided ORAddress are present in the known ORAddresses. Under-specification does not mean partial value (e.g., substring) equivalence when the same set of attributes are present in the ORAddresses.

b) Over-specified ORAddresses are not equivalent. Over-specification means that more attributes are present in the provided ORAddress than are present in the known ORAddresses.

c) An ADMD or PRMD name that is all numeric but encoded as Printable String is considered to be equivalent to the same ADMD or PRMD name, respectively, with the same numeric values encoded as Numeric String.

NOTES

1 An X.500 Directory service may or may not support these matching rules for equivalence.

2 Operational equivalence between T.61 and Printable String is for further study.

9.3 Distribution Lists

See Working Document.

9.4 MHS Use of Directory

9.4.1 Introduction

The MHS standards recognize the need of MHS users for a number of directory service elements. Directory service elements are intended to assist users, their UAs, and MTAs in obtaining information for use in submission, delivery, and the transfer of messages.

NOTE - The MTS may also use the directory service elements to obtain information, for example, to be used in the routing of messages. This application of the directory service is not defined by the base standards and is therefore not addressed by this Agreement.

9.4.2 Functional Configuration

Two MHS functional entities, the IPM UA and MTA, may access the Directory service using the Directory User Agent (DUA). The interface between the UA and DUA, or MTA and DUA is local and not defined. The interaction between the DUA and Directory System Agent (DSA) is specified in Part 11. A collocated DUA and DSA is also permitted.

9.4.3 Functionality

Examples of functional usages of directories have been identified for UAs and the MTAs in conjunction with their DUAs. These are:

a) UA Specific Functionality:

1) Verify the existence of a Directory Name;

2) Given a partial name, return a list of possibilities;

3) Search the Directory for entries containing a specified attribute type and value and return the Distinguished Names of the matching entries;

4) Return the O/R Address(es) that correspond to a Directory Name;

5) Determine whether a Directory Name presented denotes a user or a Distribution List;

6) Return the members of a Distribution List;

7) Return the capabilities of the entity referred to by a Directory Name;

8) Maintenance functions to keep the directory up-to-date, e.g., register and change credentials;

b) MTA Specific Functionality:

1) Authentication;

2) Return the O/R Address(es) that correspond to a Directory Name;

3) Determine whether a Directory Name presented denotes a user or a Distribution List;

4) Return the members of a Distribution List;

5) Return the capabilities of the entity referred to by a Directory Name;

6) Maintenance functions to keep the directory up-to-date.

In addition to functionality, a number of operational aspects must be considered. These include user-friendliness, flexibility, availability, expandability and reliability.

9.4.4 Naming and Attributes

Since user-friendliness is of primary importance in a messaging system, the naming conventions used in building the Directory Information Tree (DIT) will impact the ability of a user to make intelligent guesses for Directory Names.

It is recommended that the naming guidelines and DIT structures defined in Annex B of Recommendation X.521/ISO 9594-7 be used as the basis for MHS Directory Names. Annex C of Recommendation X.402/ISO 10021-2 specifies further the MHS specific object classes. The naming for MHS specific object classes are recommended as follows:

a) The naming for mhs-message-store, mhs-message-transfer-agent, and mhs-user-agent is that of Application Entity in the DIT.

b) The naming attribute for mhs-distribution-list is commonName. The organization, organizationalUnit, organizationalRole, organizationalPerson, locality, or groupOfNames can be immediate superior to entries of object class mhs-distribution-list.

c) The naming for mhs-user is that of organizationalPerson, residentialPerson, organizationalRole, organizationalUnit, organization, or locality.

NOTE - The mhs-user object class is a generic object class which may be used in conjunction with another standard object class for the purpose of adding MHS information attributes, such as

ORAddresses, to a Directory entry. The means to associate attributes of a generic object class to an entry (or to different entries) named by a standard object class(es) is by defining a new (un-)registered object class, whose superclass(es) is that of the naming object class(es), and of the generic object class. E.g., to associate mhs-user attributes in the organizationalPerson entry, a new unregistered object class can be defined as shown in figure 8.

```
real-user-entry  ::=  OBJECT CLASS
                      SUBCLASS OF organizationalPerson,
                                  mhs-user
```

Figure 8 - Example of Unregistered Object Class Definition.

The MHS object classes, attributes, and attribute syntaxes that need to be supported by the Directory are as specified in Annex C of Recommendation X.402/ISO 10021-2.

In addition, the object classes organization, organizationalUnit, organizationalRole, organizationalPerson, locality, groupOfNames, residentialPerson, and country and their attributes and associated syntaxes as defined in X.520 (ISO 9594, Part 6) and X.521 (ISO 9594, Part 7) are required to support the MHS.

9.4.5 Elements of Service

This clause specifies the requirements for support of Elements of Service for conformance to the Use of Directory Functional Group of this Agreement.

The classification scheme for support of Elements of Service is as defined in clause 5.2;

Support for Elements of Service is specified both for the MT Service (table 14) and for the IPM Service (table 15).

Table 14 - Use of Directory: MT Elements of Service

Element of Service	Origination	Reception	Relay
Designation of Recipient by Directory Name	M	M	-

Table 15 - Use of Directory: IPM Elements of Service

Element of Service	Origination	Reception
Designation of Recipient by Directory Name	M	-

9.4.6 Directory Services

These Implementation Agreements require the Directory services as defined in table 16. Indicated are the Directory services required to support the needs of the MHS UA/MTA and MHS Administrator.

Table 16 - Directory Service Support Requirements

Directory Service	MHS UA/MTA	MHS Admin
Bind and Unbind	M	M
Read	M	M
Compare	M	M
Abandon	M	M
List	M	M
Search	M	M
Add Entry	O	M
Remove Entry	O	M
Modify Entry	M	O
Modify RDN	O	O

9.4.7 OIW X.400 Base Directory Implementation Agreements

This clause defines the X.400 base Directory Implementation Agreements. Its structure and content are based on the Implementation Agreements template suggested in Part 11.

9.4.7.1 Other Profiles Supported

The OIW X.400 Base Directory Implementation Agreements requires the support of OIW Directory Common Application Directory Implementation Agreements as defined in Part 11.

9.4.7.2 Standard Application Specific Attributes and Attribute Sets

The standard application specific attributes and attributes sets supported by these Implementation Agreements are listed in table 17. For each attribute and attribute set, a reference is provided to the standard where it is defined.

Table 17 - Standard Attributes and Attribute Sets

Attribute / Attribute Set	References
mhs-deliverable-content-length	X.402/IS 10021-2
mhs-deliverable-content-types	X.402/IS 10021-2
mhs-deliverable-eits	X.402/IS 10021-2
mhs-dl-members	X.402/IS 10021-2
mhs-dl-submit-permissions	X.402/IS 10021-2
mhs-message-store	X.402/IS 10021-2
mhs-or-addresses	X.402/IS 10021-2
mhs-preferred-delivery-methods	X.402/IS 10021-2
mhs-supported-automatic-actions	X.402/IS 10021-2
mhs-supported-content-types	X.402/IS 10021-2
mhs-supported-optional-attributes	X.402/IS 10021-2

9.4.7.3 Standard Application Specific Object Classes

The standard application specific object classes supported by these Implementation Agreements are listed in table 18. For each object class, a reference is provided to the standard where it is defined.

Table 18 - Standard Object Classes

Object Class	References
mhs-distribution-list	X.402/IS 10021-2
mhs-message-store	X.402/IS 10021-2
mhs-message-transfer-agent	X.402/IS 10021-2
mhs-user	X.402/IS 10021-2
mhs-user-agent	X.402/IS 10021-2

9.4.7.4 OIW Application Specific Attributes and Attribute Sets

There are no application specific attributes or attribute sets defined by these Implementation Agreements.

9.4.7.5 OIW Application Specific Object Classes

There are no application specific object classes defined by these Implementation Agreements.

9.4.7.6 Structure Rules

This clause defines the naming and structure rules for the MHS object classes which are subclasses of top.

9.4.7.6.1 MHS Distribution List

Attribute commonName is used for naming.

The mhs-distribution-list, organization, organizationalUnit, organizationalRole, organizationalPerson, locality, or groupOfNames can be immediately superior to entries of object class mhs-distribution-list.

9.4.7.6.2 MHS User

The naming for mhs-user is that of organizationalPerson, residentialPerson, organizationalRole, organizationalUnit, organization, or locality.

The organizationalPerson, residentialPerson, organizationalRole, organizationalUnit, organization, or locality object classes can be combined with the mhs-user object class to form a new composite object class.

10 MHS Management

See Working Document.

11 MHS Security

11.1 Overview

The Security functional group is specified as three security classes which are incremental subsets of the security features available in the base standard. They are denoted as S0, S1, and S2. An implementation that conforms to the Security functional group map support one or more of the security classes defined in these Implementation Agreements.

S0: This security class gathers together security functions applicable only between MTS-Users. Consequently, security mechanisms are implemented within the MTS-User. An MTA is required to support the syntax of the security services on submission, as the "Kernel" supports the syntax on relay and delivery. The MTA is not expected to understand the semantics of the security services.

S1: This security class requires secure functionality with the MTS-User and MTS. The MTS secure functionality is only required to achieve secure access management. As with S0, most of the security mechanisms are implemented within an MTS-User. It primarily provides integrity and authentication between MTS-Users. However, MTAs are expected to support digital signatures for peer to peer authentication, security labelling and security contexts.

S2: This security class is a superset of S1, adding security functions within MTAs and the MTS. The main security function added within this group is authentication within the MTS, and, as a consequence, due to the non-repudiable nature of the keys used for authentication, non-repudiation is also added.

In addition, each of the three security classes has a variant, denoted as S0a, S1a, and S2a, which mandates support of end-to-end confidentiality.

Symmetric or asymmetric techniques (or a combination thereof) may be used within each security class and are identified by the registered algorithm identifier.

Various levels of assurance in trusted COMPUSEC functionality may be used within each security class. This is outside the scope of this Implementors Agreement.

A full rationale for each of the security classes and a broader discussion of security considerations are provided in annex E.

Table 19 provides an overview of the requirements made by the security classes on the MTS-User and MTA. The table entries are descriptive, and are not intended to refer to security service elements.

Table 19 - Overview of Security Requirements for Each Security Class.

	Requirements	
Class	MTS-User	MTA
Kernel		Submission, delivery, and relay of EoS
S0	Content Integrity, Proof of Delivery, Message Origin Authentication (UA to UA)	Kernel
S0a	S0 plus Content Confidentiality	Kernel
S1	S0 plus Message security label, Message security context, Security Management Services	Peer entity authentication, Security context, Security Management Services, and Message Security Label
S1a	S1 plus Content confidentiality	S1
S2	S1 plus Message Origin Authentication Check, Probe Origin Authentication Check, Report Origin Authentication Check, Proof of Submission, and, Non-repudiation	S1 plus Message Origin Authentication Check, Prove Origin Authentication Check, Report Origin Authentication Check, Proof of Submission, and, Non-repudiation
S2a	S1a plus S2	S1a plus S2

The incremental functionality of the security classes can be represented diagrammatically as shown in figure 9.

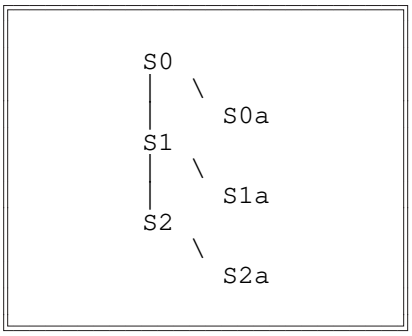

Figure 9 - Incremental Functionality of the Security Classes.

11.2 Common Requirements

11.2.1 Interworking Between Security Classes

A security class can be viewed as a tool which can be used to implement a security policy, and is not a security policy in its own right but a component of a security policy.

Interworking between implementations supporting different security classes can be achieved in terms of any common class(es) supported. As specified in the base standard, the label of the message, probe or report must be checked against the security context by any implementation claiming conformance to classes S1, S1a, S2, and S2a.

> **NOTE -** Interworking can be limited to messages of only one security class by defining a security context consisting of labels with security policy identifiers of only that security class.

This profile defines security policy identifiers (annex B, figure 15) that corresponds to the security classes defined in this section. Such generic security policy identifiers only imply support of the X.400 security services as specified for these security classes in this clause. No other COMSEC or COMPUSEC functionality can be assumed by use of such policy identifiers. More specific security policies may be based on one or more of the security classes in this section but will require use of registered policy identifiers.

11.2.2 Comparison of Security Labels

The Security Content service ensures that the message security label matches at least one of the set of labels specified in the security content established between the communicating MHS entities.

An MTA which supports the Security Content service shall as a minimum support matching for equality on the security-policy-identifier, security-classification, and security-categories elements of the label.

> **NOTE -** The basic support requirement is that absence of an element shall not be treated as "any value", i.e., all permissible combinations of occurrence and value for the elements of the message security label must be elaborated in the security context.

Any other matching rules (e.g., covering the privacy-mark element or based on alternative methods of comparison) may be used in particular application scenarios, but such specification and usage will be subject to bilateral agreement and will depend on the security policy in force.

The message security label can be placed in the per-message extensions or in the signed or encrypted data of the per-recipient message token. It is recommended that the integrity of the security label is protected by including it in the token signed data, or (if the label is in the per-message extensions) by computing the message origin authentication check on the message. (Support of MOAC is optional in security classes S0 and S1.) Which of these labels is/are checked by the security context service is dictated by the security policy in force. The security policy should also define any requirements on allowable (per-recipient) label values in the case where the message is addressed to multiple recipients (and thus has multiple tokens).

A label may also be included in the token encrypted data with (confidential) end-to-end semantics.

11.2.3 Application Context

When providing the peer entity authentication service, it is recommended that MTAs should not use the "association-recovery" procedure of RTSE (section 7.8.3 of X.228). MTAs in the role of sender should not invoke this procedure and MTAs in the role of receiver should not accept RT-OPEN requests asking for recovery.

> **NOTE -** It is permissible for the sending MTA to perform the "activity resumption" (section 7.8.1 of X.228) on an existing, authenticated RTSE association owned by this MTA.

11.3 Description of Security Classes

The sections to follow describe the security classes within the Security functional group. For each security class, there is a description of the security functionalities provided, followed by a table which gives the classification for each of the security services required by that class. Where the classification of a security service does not change for a higher security class, then that security service is not repeated in the table for the higher security class.

Figure 10 explains the column headings used in the security class tables. The classifications are defined in clause 5.2.

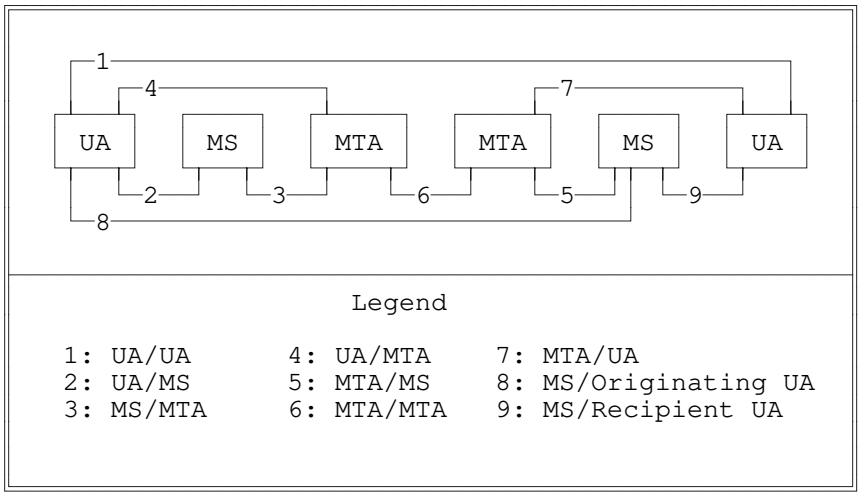

Figure 10 - Security Interfaces.

11.4 Security Class 0 (S0)

11.4.1 Security Functionality

Security measures shall be provided by the MHS implementation in order to provide the following:

a) Integrity of message content;

b) Authentication of the MTS-User who originated the message;

c) Authentication of the MTS-User to whom the message was delivered.

This security class mandates the above services are provided by an MTS-User.

There are no requirements placed on the MTA.

11.4.2 Security Services for S0

Security class 0 (S0) mandates the security services listed in table 20.

Table 20 - Security Class 0 (S0)

Security Service \ Security Interface	1 UA/ UA	2 UA/ MS	3 MS/ MTA	4 UA/ MTA	5 MTA/ MS	6 MTA/ MTA	7 MTA/ UA	8 MS/ UA	9 MS/ UA
Origin Authentication									
Message Origin Authentication[1]	M	I	–	I	–	–	–	–	–
Probe Origin Authentication	–	I[6]	–[6]	I	–	–	–	–	–
Report Origin Authentication	–	–	–	–	I	I	I	–	–
Proof of Submission	–	–	–	–	–	–	I	–	–
Proof of Delivery	M	–	–	–	–	–	–	M[4]	–
Secure Access Management									
Peer Entity Authentication[2,7]	–	O	O	O	O	O	O	–	O
Security Context	–	O	O	O	O	O	O	–	O
Data Confidentiality									
Connection Confidentiality[8]	–	I	I	I	I	I	I	–	I
Content Confidentiality	I	–	–	–	–	–	–	–	–
Message Flow Confidentiality	I	–	–	–	–	–	–	–	–
Data Integrity Services									
Connection Integrity[8]	–	I	I	I	I	I	I	–	I
Content Integrity	M	–	–	–	–	–	–	–	–
Message Sequence Integrity[11]	O	–	–	–	–	–	–	–	–
Non-Repudiation									
Non-Repudiation of Origin[1,5]	O	–	–	I	–	–	–	–	–
Non-Repudiation of Submission	–	–	–	–	–	–	I	–	–
Non-Repudiation of Delivery[5,10]	O	–	–	–	–	–	–	O	–
Message Security Labelling[2,3]	O	O	O	O	O	O	O	O	O
Security Management Services									
Change Credentials	–	O	–	O	O	I[9]	O	–	–
Register	–	O	–	O	–	–	–	–	–
MS-Register	–	O	–	–	–	–	–	–	–

Table 20 - Security Class 0 (S0) (concluded)

Notes
1 Only provided to the message recipient.
2 Using either symmetric or asymmetric algorithms as identified by the algorithm identifier in the applicable protocol element.
3 When security labelling is used, the security policy identifier shall be included.
4 If Proof of Delivery and Content Confidentiality are both used, and delivery is to an MS, then proof of delivery can only be computed on the encrypted content. It should be noted that this will not provide non-repudiation of delivery.
5 Using either a trusted notary (symmetric) or using certificates tokens which are not repudiable (asymmetric).
6 Corrects table 7 of X.402 in the base standard.
7 Authentication between collocated objects is a local issue.
8 Refer to section 10 of X.402 and ISO/IEC 10 021-2 and IS 7498-2.
9 These services are expected to be provided by non-standard management services and are therefore outside the scope of this Implementors Agreement.
10 Non-Repudiation of Delivery can only be provided when the proof-of-delivery service is used.
11 Allocation and management of sequence numbers is outside the of this Implementors Agreement (as it is subject to bilateral agreements).

11.5 Security Class 0A (S0a)

11.5.1 Security Functionality

Security measures shall be provided by the MHS Implementation in order to provide the following:

a) Security Functionality defined in security class S0;

b) Content Confidentiality.

11.5.2 Security Services for S0a

Security class 0A (S0a) mandates the security services of class S0 plus those listed in table 21.

Table 21 - Security Class 0A (S0a)

Security Interface / Security Service	1 UA/ UA	2 UA/ MS	3 MS/ MTA	4 UA/ MTA	5 MTA/ MS	6 MTA/ MTA	7 MTA/ UA	8 MS/ UA	9 MS/ UA
Data Confidentiality Content Confidentiality	M	–	–	–	–	–	–	–	–

11.6 Security Class 1 (S1)

11.6.1 Security Functionality

Security measures shall be provided by the MHS implementation in order to provide the following:

a) Authentication of MTA, MS, and UA;

b) Confidentiality of connections between MTA, MS, and UA;

c) Integrity of message content;

d) Authentication of message originator;

e) Authentication of message delivery (Proof of delivery);

f) MLS-features of MTA, MS, and UA;

g) MLS-separation of messages, probes, and reports;

h) MLS-mediation by secure access measures.

NOTES

1 The level of assurance of the MLS trusted components is subject to bilateral agreement.

2 The level of accountability provided is subject to bilateral agreement.

11.6.2 Security Services for S1

Security class 1 (S1) mandates the security services of class S0 plus those listed in table 22.

Table 22 - Security Class 1 (S1)

Security Interface / Security Service	1 UA/ UA	2 UA/ MS	3 MS/ MTA	4 UA/ MTA	5 MTA/ MS	6 MTA/ MTA	7 MTA/ UA	8 MS/ UA	9 MS/ UA
Origin Authentication									
Message Origin Authentication[2]	M[1]	I	–	I	–	–	–	–	–
Secure Access Management									
Peer Entity Authentication[3,4]	–	M[1]	M[1]	M[1]	M[1]	M[1]	M[1]	–	M[1]
Security Context	–	M[1]	M[1]	M[1]	M[1]	M[1]	M[1]	–	M[1]
Data Integrity Services									
Content Integrity	M[1]	–	–	–	–	–	–	–	–
Message Security Labelling[3]	M[1]	M[1]	M[1]	M[1]	M[1]	M[1]	M[1]	M[1]	M[1]
Security Management Services									
Change Credentials	–	M	–	M	M	I[5]	M	–	–
Register	–	M	–	M	–	–	–	–	–
MS-Register	–	M	–	–	–	–	–	–	–

Notes
1 Shall always be used.
2 Only provided to the message recipient.
3 Using either symmetric or asymmetric algorithms as identified by the algorithm identifier in the applicable protocol element.
4 Authentication between collocated objects is a local issue.
5 These services are expected to be provided by non-standard management services and are therefore outside the scope of this Implementors Agreement.

11.7 Security Class 1A (S1a)

11.7.1 Security Functionality

Security measures shall be provided by the MHS implementation in order to provide the following:

a) Security functionality defined for security class S1;

b) Content Confidentiality.

11.7.2 Security Services for S1a

Security class 2A (S1a) mandates the security services of class S1 plus those listed in table 23.

Table 23 - Security Class 1A (S1a)

Security Interface / Security Service	1 UA/ UA	2 UA/ MS	3 MS/ MTA	4 UA/ MTA	5 MTA/ MS	6 MTA/ MTA	7 MTA/ UA	8 MS/ UA	9 MS/ UA
Data Confidentiality Content Confidentiality	M	–	–	–	–	–	–	–	–

11.8 Security Class 2 (S2)

11.8.1 Security Functionality

Security measures shall be provided by the MHS implementation in order to provide the following:

a) Security functionality defined for security class S1;

b) Authentication and non-repudiation of messages, probes, and reports.

11.8.2 Security Service for S2

Security class 2 (S2) mandates the security services of class S1 plus those listed in table 24.

Table 24 - Security Class 2 (S2)

Security Interface / Security Service	1 UA/ UA	2 UA/ MS	3 MS/ MTA	4 UA/ MTA	5 MTA/ MS	6 MTA/ MTA	7 MTA/ UA	8 MS/ UA	9 MS/ UA
Origin Authentication									
Message Origin Authentication[3]	M[1]	M[1]	–	M[1]	–	–	–	–	–
Probe Origin Authentication	–	M[4]	–	M[1]	–	–	–	–	–
Report Origin Authentication	–	–	–	–	M[1]	M[1]	M[1]	–	–
Proof of Submission	–	–	–	–	–	–	–	M	–
Non-Repudiation									
Non-Repudiation of Origin	M[5]	–	–	M[2]	–	–	–	–	–
Non-Repudiation of Submission	–	–	–	–	–	–	M[2]	–	–
Non-Repudiation of Delivery	M[5]	–	–	–	–	–	–	M[2]	–

Notes
1 Shall always be used.
2 Using an asymmetric mechanism (i.e., certificates and tokens which are not repudiable for authentication within MTAs and the MTS.
3 Using the Message Origin Authentication Check as detailed in the base standard.
4 Shall always be used, and corrects table 7 in X.402.
5 Using either a trusted notary (symmetric) or using certificates tokens which are not repudiable (asymmetric).

11.9 Security Class 2A (S2a)

11.9.1 Security Functionality

Security measures shall be provided by the MHS implementation in order to provide the following:

a) Security functionality defined for security class S2;

b) Content Confidentiality.

11.9.2 Security Services for S2a

Security class 2A (S2a) mandates the services of class S2 plus those listed in table 25.

Table 25 - Security Class 2A (S2a)

Security Interface / Security Service	1 UA/ UA	2 UA/ MS	3 MS/ MTA	4 UA/ MTA	5 MTA/ MS	6 MTA/ MTA	7 MTA/ UA	8 MS/ UA	9 MS/ UA
Data Confidentiality Content Confidentiality	M	–	–	–	–	–	–	–	–

12 Specialized Access

See Working Document.

13 Conversion

See Working Document.

14 Redirection

See Working Document.

15 EDI Messaging Service

See Working Document.

16 Use of Underlying Layers

16.1 MTS Transfer Protocol (P1)

The P1 protocol is mapped onto the Reliable Transfer Service Element (RTSE) either in X.410-1984 mode or in normal mode, as specified in clause 5.3. In X.410-1984 mode, the RTSE makes direct use of the services provided by the Session Layer, as specified in Part 5 (Upper Layers) of the Stable Implementation Agreements. In normal mode, the RTSE makes use of the services provided by the Association Control Service Element (ACSE) and Presentation Layer, as defined in Part 5 (Upper Layers) of these Agreements.

16.2 MTS Access Protocol (P3) and MS Access Protocol (P7)

The P3 and P7 protocols make use of the services provided by the Remote Operations Service Element (ROSE), Association Control Service Element (ACSE), Presentation Layer, and, optionally, the Reliable Transfer Service Element (RTSE), as defined in Part 5 (Upper Layers) of these Agreements. It is recommended that RTSE be used for recovery purposes when the implementation does not use Transport Class 4 or there is a high probability of an association failure.

17 Error Handling

This clause describes appropriate actions to be taken upon receipt of protocol elements which are not supported in these Implementation Agreements: malformed PDUs, unrecognized O/R Name forms, content errors, errors in reports, and unexpected values for protocol elements.

An implementation must be able to report all error conditions which may occur with the appropriate error information as defined in the referenced base standards. An implementation must be able to handle receipt of all error indications which are defined in the referenced base standards. An implementation must also be tolerant of any additional error indications which are not currently defined, but is not required to be able to interpret such error information.

17.1 PDU Encoding

See Working Document.

17.2 Contents

See Working Document.

17.3 Envelope

See Working Document.

17.4 Reports

See Working Document.

17.5 Pragmatic Constraints

See Working Document.

18 Conformance

For this clause, the term *conformance* is as defined in ISO 9646.

Bilateral agreements between domains may be implemented in addition to the requirements stated in this document. **Conformance to this Agreement requires the ability to exchange messages without use of bilateral agreements**.

In order to achieve a more precise definition of conformance requirements according to the functionality supported by an implementation, the concept of Functional Groups has been introduced. A Functional Group is a set of related Elements of Service and associated protocol elements which provide a discrete area of functionality.

Conformance to this Agreement requires as a minimum that all Mandatory Elements of Service listed in this Part are supported in the manner defined in the MHS standards, as qualified in this Agreement, for each of the Functional Groups claimed. Any Optional Elements of Service for which support is claimed must also be supported as defined in the MHS standards and as qualified in this Agreement. Pragmatic constraints shall be observed as specified in the CCITT X.400 (1988) Series of Recommendations. It is not necessary to implement the recommended practices of annex D in order to claim conformance to this Agreement.

Conformance requirements for support of Functional Groups by particular configuration types (see clause 2) are listed in table 32. An implementation may claim conformance to multiple configuration

types (e.g., "MTA+UA" and "Class B MTA only").

Table 32 - Conformance Requirements

	Configuration[3]								
	MTA + UA[2]	MTA + MS	MTA Only[1]			MS + UA	MS Only	UA Only	
Functional Group			A	B	C			P7	P3
MT Kernel	M[2]	M	M	M	M	–	–	–	–
IPM Kernel	M	–	–	–	–	M	–	M	M
Message Store[4]	–	M	–	–	–	M	M	M	–
Remote UA	O	O	–	M	–	–	–	–	M
Distribution List	O	O	O	O	O	*	–	*	*
Directory	O	O	O	O	O	O	O	O	O
MHS Management	*	*	*	*	*	*	*	*	*
Security	O	O	O	O	O	O	O	O	O
Physical Delivery	*	*	*	*	*	*	*	*	*
Other Access Units	*	*	*	*	*	*	*	*	*
Conversion	*	*	*	*	*	*	*	*	*
Redirection	*	*	*	*	*	*	*	*	*
EDI Messaging	*	*	*	*	*	*	*	*	*

Notes

1 There are three conformance levels defined for the MT Kernel in clause 18.1.

2 Optional elements of the IPM Kernel need not be supported in the MT Kernel in this configuration, for example Probe and Deferred Delivery Cancellation.

3 The designation of a '+' in a configuration (e.g., 'MTA+MS') implies that there is no exposed protocol in the interface between the two components.

4 There are two conformance levels defined in clause 18.2 for MS support.

18.1 MT Kernel Conformance Levels

The MT Kernel conformance levels are:

a) A class 'A' MT Kernel implementation conveys a message, probe, or report to another MT Kernel using standard means. A class 'A' MT Kernel is specifically implemented in order to transfer messages, probes, and reports which have previously been transferred and need not support submission and delivery. A class 'A' MT Kernel may perform other activities such as originate reports, expand distribution lists, and perform conversions.

b) A class 'B' MT Kernel implementation supports submission, delivery, and transfer using standard means, i.e. P3 and P1. A class 'B' MT Kernel need not support the transfer of previously transferred messages, probes, or reports.

c) A class 'C' MT Kernel implementation requires support for transfer of messages, probes, and reports to another MT Kernel using standard means. A class 'C' MT Kernel does not

require support for the transfer of previously transferred messages, probes, and reports, and message submission and delivery is achieved by non-standard means.

An MTA may conform to one or more of the MT Kernel classes. For example, a class ‘B’ or ‘C’ MT Kernel which supports the transfer of previously transferred messages, probes, and reports is also conformant to a class ‘A’ MT Kernel. Figure 11 illustrates several combinations of MT Kernel conformance classes. Additional combinations are possible.

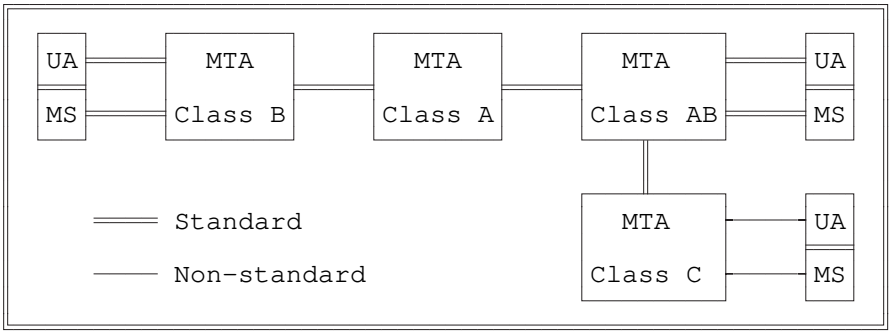

Figure 11 - MT Kernel Conformance Classes

18.2 MS Conformance Levels

The MS conformance levels are:

a) A Basic MS only requires support for the General Attributes as specified in clause 8 of annex A;

b) An IPM MS requires support from both the General Attributes and IPM Attributes as specified in clauses 8 and 10, respectively, of annex A.

19 Management Domain Agreements

See Working Document.

Annex A (normative)

MHS Protocol Specifications

Tables 34 through 49 specify the requirements for support of MHS protocol elements for conformance to this Agreement. It should be noted that the tables specify minimum support for conformance to the relevant Kernel functional groups and where appropriate also specify enhanced support requirements where one or more further functional groups are claimed. **All element support is subject to further review and may be upgraded in later versions of this Agreement**.

Within the classification tables (34-49), the column "S" indicates the classification from the base standards. This is provided for reference purposes only and is intended to be in agreement with the base standards.

The protocol support classification scheme used in this version of this Agreement is described below. **However, it should be noted that the scheme is currently under review both within the OIW X.400 SIG and in the EWOS/ETSI MHS groups and is likely to be revised for later versions of this Agreement**.

The classification of support for a protocol element specifies the requirements for implementations conforming to this Agreement to be able to generate, receive and process that protocol element, as appropriate (the 'receiving' role includes relaying where appropriate). The classification of support for each protocol element is relative to that for its containing element. Where sub-elements within a containing element are not listed, then their support classification shall be assumed to be that of the containing element. Where the range of values to be supported for an element is not specified, then all values defined in the base standard shall be supported.

The classifications have been revised. The new classifications relate to the classifications in the Part 7 of the Stable Agreements as shown in table 33.

Table 33 - Classification Changes

	New	
Former Category	Originator Category	Recipient Category
Generatable (G)	Mandatory (M)	Mandatory (M)
Supported (H)	Optional (O)	Mandatory (M)
Mandatory (M)	Mandatory (M)	Mandatory (M)
Required (R)	Mandatory (M)	Mandatory (M)
Unsupported (X)	Optional (O)	Optional (O)

The support classifications are stated for both Origination and Reception (O/R) in the following tables (34-49). The defined support for each is stated within each classification.

Implementations conforming to this Agreement must be capable of accepting the syntax of every protocol element of a protocol for which support is claimed. When an MS or MTA receives a protocol element that according to the base standard should be conveyed to another MHS entity (MTA, MS, or

UA), the MS or MTA is required to preserve the semantics of that protocol element in the PDU conveyed. Notwithstanding the above, criticality must be observed according to the base standard.

Mandatory (M) on Origination: Implementations conforming to this Agreement shall generate this element in all information objects in which, according to the base standards, it shall occur.

Mandatory (M) on Reception: Implementations conforming to this Agreement shall process this element appropriately according to its semantics.

Optional (O) on Origination: Where this element is not conveyed from one MHS entity to another, implementations conforming to this Agreement may optionally be capable of generating this protocol element, but are not required to do so.

Optional (O) on Reception: Implementations conforming to this Agreement may, but are not required to be capable of processing this protocol element.

NOTE - Some protocol elements may not be conveyed, if downgrading rules are applied.

To Be Determined (*): the support classification for this protocol element has yet to be determined.

Not Applicable (-): The protocol element is not applicable in the particular context according to the base standard.

Where the dynamic behavior of protocol elements need to be specified, the following classification scheme is used:

Mandatory (m): The protocol element shall always be implemented and generated. On reception, correct action shall be taken as specified in the base standard, or as qualified or specified in these Agreements. Absence of the corresponding protocol element shall cause the appropriate abstract error to be generated.

Excluded (x): The protocol element shall not be present or it must be possible to prevent its use. Its presence shall cause the appropriate abstract error to be generated.

Dynamic conformance classifications are indicated in a single column of each of the Protocol Element tables. The classification applies to the usage only of the protocol elements which have a static classification.

A.1 MTS Transfer Protocol (P1)

Table 34 - Classification of the P1 Protocol Elements

MTS Transfer Protocol (P1)				Part 1 of 9
	MT Kernel Support by MTS Class			Comments/References
Protocol Element	S	B/C O/R	A O/R	See Note 1
Operations				
MTABind	M	M/M	M/M	MTABind
MTAUnbind	M	M/M	M/M	
MTSE				See protocol elements
MessageTransfer	M	M/M	M/M	
ProbeTransfer	M	M/M	M/M	
ReportTransfer	M	M/M	M/M	
Arguments/Results				
MTABind				
ARGUMENT				
<NULL>	O	O/M	O/M	See Note 2
<SET>	O	M/M	M/M	
initiator-name	M	M/M	M/M	
initiator-credentials	M	M/M	M/M	
simple	O	M/M	M/M	
strong	O	O/O	O/O	
security-context	O	O/O	O/O	
RESULT				
<NULL>	O	O/M	O/M	See Note 2
<SET>	O	M/M	M/M	
responder-name	M	M/M	M/M	
responder-credentials	M	M/M	M/M	
simple	O	M/M	M/M	
strong	O	O/O	O/O	

Notes

1 The MT Kernel implementation classes are defined in clause 16.

2 The action to be taken on receipt of null MTABind authentication is that an implementation must understand the semantics, but the form of authentication that is acceptable is a local matter.

Table 34 - Classification of the P1 Protocol Elements (continued)

MTS Transfer Protocol (P1)				Part 2 of 9
	MT Kernel Support by MTS Class			Comments/References
Protocol Element	S	B/C O/R	A O/R	See Note 1
MTS-APDU				
message	M	M/M	O/M	
envelope	M	M/M	M/M	MessageTransferEnvelope
content	M	M/M	M/M	See P2 - else undefined
probe	M	M/M	O/M	ProbeTransferEnvelope
report	M	M/M	M/M	
envelope	M	M/M	M/M	ReportTransferEnvelope
content	M	M/M	M/M	ReportTransferContent
MessageTransferEnvelope				
message-identifier	M	M/M	M/M	MTSIdentifier
originator-name	M	M/M	M/M	ORName
original-encoded-information-types	O	M/M	O/O	EncodedInformationTypes
content-type	M	M/M	M/M	
built-in	O	M/M	O/O	
external	O	O/M	O/O	
content-identifier	O	O/M	O/O	
priority	O	M/M	O/M	All values
per-message-indicators	O	M/M	O/M	
disclosure-of-recipients	O	O/M	O/M	
implicit-conversion-prohibited	O	M/M	O/M	
alternate-recipient-allowed	O	M/M	O/O	
content-return-request	O	O/O	O/O	
deferred-delivery-time	O	O/O	O/O	
per-domain-bilateral-information	O	O/O	O/O	PerDomainBilateralInfo
trace-information	M	M/M	M/M	TraceInformation
extensions	O	M/M	M/M	ExtensionField
recipient-reassignment-prohibited	O	M/M	M/M	
dl-expansion-prohibited	O	M/M	O/M	
conversion-with-loss-prohibited	O	O/M	O/M	
latest-delivery-time	O	O/O	O/O	See X.411, 14.1.1 note 2
originator-return-address	O	O/O	O/O	
originator-certificate	O	O/O	O/O	
content-confidentiality-algorithm-identifier	O	M/M	M/M	See Note 6
message-origin-authentication-check	O	O/O	O/O	
message-security-label	O	O/O	O/O	See Note 5
security-policy-identifier	O	M/M	M/M	
security-classification	O	M/M	M/M	
privacy-mark	O	O/O	O/O	
security-categories	O	M/M	M/M	
content-correlator	O	O/O	O/O	

Table 34 - Classification of the P1 Protocol Elements (continued)

MTS Transfer Protocol (P1)				Part 3 of 9
	MT Kernel Support by MTS Class			Comments/References
Protocol Element	S	B/C O/R	A O/R	See Note 1
dl-expansion-history	O	O/M	O/M	DLExpansionHistory
internal-trace-information	O	M/M	M/M	InternalTraceInfo
per-recipient-fields	M	M/M	M/M	
recipient-name	M	M/M	M/M	ORName
originally-specified-recipient-number	M	M/M	M/M	
per-recipient-indicators	M	M/M	M/M	
explicit-conversion	O	O/O	O/O	
extensions	O	O/M	O/M	ExtensionField
originator-requested-alternate-recipient	O	O/O	O/O	
requested-delivery-method	O	M/M	O/M	
physical-forwarding-prohibited	O	O/O	O/O	
physical-forwarding-address-request	O	O/O	O/O	
physical-delivery-modes	O	O/O	O/O	
registered-mail-type	O	O/O	O/O	
recipient-number-for-advice	O	O/O	O/O	
physical-rendition-attributes	O	O/O	O/O	
physical-delivery-report-request	O	O/O	O/O	
message-token	O	O/O	O/O	
asymmetric-token	O	M/M	M/M	See Note 5
signature-algorithm-identifier	M	M/M	M/M	
name	M	M/M	M/M	
time	M	M/M	M/M	
sign-data	O	M/M	M/M	
content-confidentiality-algorithm-identifier	O	M/M	M/M	
content-integrity-check	O	M/M	M/M	
message-security-label	O	O/O	O/O	
proof-of-delivery-request	O	M/M	M/M	
message-sequence-number	O	O/O	O/O	
encryption-algorithm-identifier	O	M/M	M/M	
encrypted-data	O	M/M	M/M	
content-confidentiality-key	O	M/M	M/M	
content-integrity-check	O	M/M	M/M	
message-security-label	O	O/O	O/O	
content-integrity-key	O	O/O	O/O	
message-sequence-number	O	O/O	O/O	
content-integrity-check	O	M/M	M/M	See Note 6
proof-of-delivery-request	O	M/M	M/M	See Note 6
redirection-history	O	O/M	O/M	

Table 34 - Classification of the P1 Protocol Elements (continued)

MTS Transfer Protocol (P1)				Part 4 of 9
	MT Kernel Support by MTS Class			Comments/References
Protocol Element	S	B/C O/R	A O/R	See Note 1
ProbeTransferEnvelope				
probe-identifier	M	M/M	M/M	MTSIdentifier
originator-name	M	M/M	M/M	ORName
original-encoded-information-types	O	M/M	O/O	EncodedInformationTypes
content-type	M	M/M	M/M	
built-in	O	M/M	O/O	
external	O	O/M	O/O	
content-identifier	O	O/M	O/O	
content-length	O	M/M	O/O	
per-message-indicators	O	M/M	O/M	
disclosure-of-recipients	O	O/O	O/O	
implicit-conversion-prohibited	O	M/M	O/M	
alternate-recipient-allowed	O	M/M	O/O	
content-return-request	O	O/O	O/O	
per-domain-bilateral-information	O	O/O	O/O	PerDomainBilateralInfo
trace-information	M	M/M	M/M	TraceInformation
extensions	O	M/M	M/M	ExtensionField
recipient-reassignment-prohibited	O	O/O	O/O	
dl-expansion-prohibited	O	M/M	O/M	
conversion-with-loss-prohibited	O	O/O	O/O	
originator-certificate	O	O/O	O/O	
message-security-label	O	O/O	O/O	
content-correlator	O	O/O	O/O	
probe-origin-authentication-check	O	O/O	O/O	
dl-expansion-history	O	O/M	O/M	DLExpansionHistory
internal-trace-information	O	M/M	M/M	InternalTraceInfo
per-recipient-fields	M	M/M	M/M	
recipient-name	M	M/M	M/M	ORName
originally-specified-recipient-number	M	M/M	M/M	
per-recipient-indicators	M	M/M	M/M	
explicit-conversion	O	O/O	O/O	
extensions	O	O/M	O/M	ExtensionField
originator-requested-alternate-recipient	O	O/O	O/O	
requested-delivery-method	O	M/M	O/M	
physical-rendition-attributes	O	O/O	O/O	
redirection-history	O	O/M	O/M	

Table 34 - Classification of the P1 Protocol Elements (continued)

MTS Transfer Protocol (P1)				Part 5 of 9
	MT Kernel Support by MTS Class			Comments/References
Protocol Element	S	B/C O/R	A O/R	See Note 1
ReportTransferEnvelope				
report-identifier	M	M/M	M/M	MTSIdentifier
report-destination-name	M	M/M	M/M	ORName
trace-information	M	M/M	M/M	TraceInformation
extensions	O	M/M	M/M	ExtensionField
message-security-label	O	O/O	O/O	
originator-and-DL-expansion-history	O	M/M	O/O	OriginatorAndDL ExpansionHistory
reporting-DL-name	O	O/O	O/O	
reporting-MTA-certificate	O	O/O	O/O	
report-origin-authentication-check	O	O/O	O/O	
internal-trace-information	O	M/M	M/M	InternalTraceInfo
ReportTransferContent				
subject-identifier	M	M/M	M/M	MTSIdentifier
subject-intermediate-trace-information	O	M/M	M/M	TraceInformation
original-encoded-information-types	O	M/M	M/M	EncodedInformationTypes
content-type	O	M/M	M/M	
built-in	O	M/M	M/M	
external	O	M/M	M/M	
content-identifier	O	M/M	M/M	
returned-content	O	O/M	O/O	
additional-information	O	O/O	O/O	
extensions	O	O/M	O/M	ExtensionField
content-correlator	O	O/M	O/M	
per-recipient-fields	M	M/M	M/M	
actual-recipient-name	M	M/M	M/M	ORName
originally-specified-recipient-number	M	M/M	M/M	

Table 34 - Classification of the P1 Protocol Elements (continued)

MTS Transfer Protocol (P1)				Part 6 of 9
	MT Kernel Support by MTS Class			Comments/References
Protocol Element	S	B/C O/R	A O/R	See Note 1
per-recipient-indicators	M	M/M	M/M	
last-trace-information	M	M/M	M/M	
arrival-time	M	M/M	M/M	
converted-encoded-information-types	O	M/M	M/M	EncodedInformationTypes
report	M	M/M	M/M	
delivery	O	M/M	O/O	
message-delivery-time	O	M/M	M/M	
type-of-MTS-user	O	M/M	O/O	All values =O/M
non-delivery	O	M/M	M/M	
non-delivery-reason-code	O	M/M	M/M	
non-delivery-diagnostic-code	O	O/M	O/M	
originally-intended-recipient-name	O	M/M	M/M	ORName
supplementary-information	O	O/O	O/O	
extensions	O	M/M	M/M	ExtensionField
redirection-history	O	M/M	M/M	RedirectionHistory
physical-forwarding-address	O	O/O	O/O	
recipient-certificate	O	O/O	O/O	
proof-of-delivery	O	O/O	O/O	
Common Data Types				
EncodedInformationTypes				
built-in-encoded-information-types	M	M/M	M/M	See Note 3
non-basic-parameters	O	O/O	O/O	
external-encoded-information-types	O	O/M	O/M	
MTSIdentifier				
global-domain-identifier	M	M/M	M/M	GlobalDomainIdentifier
local-identifier	M	M/M	M/M	
PerDomainBilateralInfo				
country-name	M	M/M	M/M	
administration-domain-name	O	M/M	M/M	DomainName
private-domain-identifier	O	M/M	M/M	DomainName (only encoded as SEQ if both present)
bilateral-information	M	M/M	M/M	

Table 34 - Classification of the P1 Protocol Elements (continued)

MTS Transfer Protocol (P1)				Part 7 of 9
	MT Kernel Support by MTS Class			Comments/References
Protocol Element	S	B/C O/R	A O/R	See Note 1
TraceInformation				
TraceInformationElement	M	M/M	M/M	
global-domain-identifier	M	M/M	M/M	GlobalDomainIdentifier
domain-supplied-information	M	M/M	M/M	
arrival-time	M	M/M	M/M	
routing-action	M	M/M	M/M	
relayed	O	M/M	M/M	
rerouted	O	O/M	O/M	
attempted-domain	O	O/M	O/M	GlobalDomainIdentifier
deferred-time	O	M/M	M/M	
converted-encoded-information-types	O	O/M	O/M	EncodedInformationTypes
other-actions	O	O/M	O/M	
redirected	O	O/M	O/M	
dl-operation	O	O/M	O/M	
ExtensionField				
type	M	M/M	M/M	
criticality	O	O/M	O/M	
for-submission	O	O/O	O/O	
for-transfer	O	M/M	M/M	
for-delivery	O	M/M	M/M	
value	M	M/M	M/M	
DLExpansionHistory				
DLExpansion	M	M/M	M/M	
ORAddressAndOptionalDirectoryName	M	M/M	M/M	ORName
dl-expansion-time	M	M/M	M/M	
InternalTraceInformation				
InternalTraceInformationElement	M	M/M	M/M	
global-domain-identifier	M	M/M	M/M	GlobalDomainIdentifier
mta-name	M	M/M	M/M	
mta-supplied-information	M	M/M	M/M	
arrival-time	M	M/M	M/M	
routing-action	M	M/M	M/M	
relayed	O	M/M	M/M	
rerouted	O	O/M	O/M	
attempted	O			
mta	O	O/M	O/M	
domain	O	O/M	O/M	GlobalDomainIdentifier
deferred-time	O	O/M	O/M	
other-actions	O	O/M	O/M	
redirected	O	O/M	O/M	
dl-operation	O	O/M	O/M	
OriginatorAndDLExpansionHistory				
originator-or-dl-name	M	M/M	M/M	
origination-or-expansion-time	M	M/M	M/M	

Table 34 - Classification of the P1 Protocol Elements (continued)

MTS Transfer Protocol (P1)				Part 8 of 9
	MT Kernel Support by MTS Class			Comments/References
Protocol Element	S	B/C O/R	A O/R	See Note 1
RedirectionHistory				
Redirection	M	M/M	M/M	
intended-recipient-name	M	M/M	M/M	
ORAddressAndOptionalDirectory Name	M	M/M	M/M	ORName
redirection-time	M	M/M	M/M	
redirection-reason	M	M/M	M/M	
ORName				
address	M	M/M	M/M	
standard-attributes	M	M/M	M/M	
country-name	O	M/M	O/M	CountryName
administration-domain-name	O	M/M	O/M	DomainName
network-address	O	M/M	O/M	
terminal-identifier	O	M/M	O/M	
private-domain-name	O	M/M	O/M	DomainName
organization-name	O	M/M	O/M	
numeric-user-identifier	O	M/M	O/M	
personal-name	O	M/M	O/M	
surname	M	M/M	M/M	
given-name	O	M/M	O/M	
initials	O	M/M	O/M	See Note 4
generation-qualifier	O	M/M	O/M	
organizational-unit-names	O	M/M	O/M	
OrganizationUnitName	M	M/M	O/M	
domain-defined-attributes	O	M/M	O/M	
DomainDefinedAttribute	M	M/M	O/M	
type	M	M/M	M/M	
value	M	M/M	M/M	
extension-attributes	O	O/M	O/M	ExtensionAttribute
common-name	O	O/M	O/M	
teletex-common-name	O	O/M	O/M	
teletex-organization-name	O	M/M	O/M	
teletex-personal-name	O	M/M	O/M	
teletex-organizational-unit-names	O	M/M	O/M	
teletex-domain-defined-attributes	O	M/M	O/M	
pds-name	O	O/M	O/M	
physical-delivery-country-name	O	O/M	O/M	
postal-code	O	O/M	O/M	
physical-delivery-office-name	O	O/M	O/M	

Table 34 - Classification of the P1 Protocol Elements (concluded)

MTS Transfer Protocol (P1)				Part 9 of 9
	MT Kernel Support by MTS Class			Comments/References
Protocol Element	S	B/C O/R	A O/R	See Note 1
physical-delivery-office-number	O	O/M	O/M	
extension-OR-address-components	O	O/M	O/M	
physical-delivery-personal-name	O	O/M	O/M	
physical-delivery-organization-name	O	O/M	O/M	
extension-physical-delivery-address-components	O	O/M	O/M	
unformatted-postal-address	O	O/M	O/M	
street-address	O	O/M	O/M	
post-office-box-address	O	O/M	O/M	
poste-restante-address	O	O/M	O/M	
unique-postal-name	O	O/M	O/M	
local-postal-attributes	O	O/M	O/M	
extended-network-address	O	O/M	O/M	
terminal-type	O	O/M	O/M	
directory-name	O	O/O	O/O	
ExtensionAttribute				
extension-attribute-type	M	M/M	M/M	
extension-attribute-value	M	M/M	M/M	
GlobalDomainIdentifier				
country-name	M	M/M	M/M	CountryName
administration-domain-name	M	M/M	M/M	DomainName
private-domain-identifier	O	M/M	O/M	DomainName
CountryName				
x121-dcc-code	O	O/M	O/M	
iso-3166-alpha2-code	O	M/M	O/M	
DomainName				
numeric	O	O/M	O/M	
printable	O	M/M	O/M	

Notes (continued)

3 An implementation is only required to generate EITs that correspond to the body parts it is capable of generating.

4 If the initials component of personal-name attribute is used, it should comprise all of the person's initials (including the given name) except the person's surname, as specified in X.402/IS 10021-2.

5 All S0 services may be provided without using the message token, e.g., using per-message extensions.

A.2 Interpersonal Messaging Protocol (P2)

Table 35 - Classification of the P2 Protocol Elements

Interpersonal Messaging Protocol (P2)			Part 1 of 3
	Support by UA		
Protocol Element	S	O/R	Comments/References
InformationObject			
ipm	O	M/M	IPM
ipn	O	M/M	IPN - see Note 4
IPM			
heading	M	M/M	
this-IPM	M	M/M	IPMIdentifier
originator	O	M/M	ORDescriptor
authorizing-users	O	O/M	RecipientSpecifier
primary-recipients	O	M/M	RecipientSpecifier
copy-recipients	O	M/M	RecipientSpecifier
blind-copy-recipients	O	O/M	RecipientSpecifier
replied-to-IPM	O	M/M	IPMIdentifier
obsoleted-IPMs	O	O/M	IPMIdentifier
related-IPMs	O	O/M	IPMIdentifier
subject	O	M/M	See Note 1, 8
expiry-time	O	O/M	
reply-time	O	O/M	
reply-recipients	O	O/M	ORDescriptor
importance	O	O/M	
sensitivity	O	O/M	
auto-forwarded	O	O/M	
extensions	O	O/M	HeadingExtension
incomplete-copy	O	O/O	
languages	O	O/M	
body	M	M/M	BodyPart
IPN			
common-fields	M	M/M	
subject-ipm	M	M/M	
ipn-originator	O	M/M	ORDescriptor
ipm-preferred-recipient	O	M/M	ORDescriptor
conversion-eits	O	O/M	EncodedInformationTypes
non-receipt-fields	O	M/M	See Note 5
non-receipt-reason	M	M/M	
discard-reason	O	M/M	
auto-forward-comment	O	O/M	
returned-ipm	O	O/O	See Note 2
receipt-fields	O	O/M	
receipt-time	M	M/M	

Table 35 - Classification of the P2 Protocol Elements (continued)

Interpersonal Messaging Protocol (P2)			Part 2 of 3
	Support by UA		
Protocol Element	S	O/R	Comments/References
acknowledgment-mode	O	O/M	
suppl-receipt-info	O	O/O	
HeadingExtension			
type	M	M/M	
value	M	M/M	
IPMIdentifier			
user	O	O/M	
user-relative-identifier	M	M/M	
ORDescriptor			
formal-name	O	O/M	ORName - see Note 3
free-form-name	O	O/M	See Note 8
telephone-number	O	O/M	
RecipientSpecifier			
recipient	M	M/M	ORDescriptor
notification-requests	O	O/M	
reply-requested	O	O/M	
BodyPart			
ia5-text	O	M/M	
parameters	M	M/M	
repertoire	O	O/M	See Note 6
data	M	M/M	
voice	O	*	See Note 7
g3-facsimile	O	O/O	
parameters	M	M/M	
number-of-pages	O	O/M	
non-basic-parameters	O	O/M	
data	M	M/M	
g4-class1	O	O/O	
teletex	O	O/O	
parameters	M	M/M	
number-of-pages	O	O/O	
telex-compatible	O	O/O	
non-basic-parameters	O	O/O	
data	M	M/M	
videotex	O	O/O	
parameters	M	M/M	
syntax	O	O/M	
data	M	M/M	
encrypted	O	*	See Note 7

Table 35 - Classification of the P2 Protocol Elements (concluded)

Interpersonal Messaging Protocol (P2)			Part 3 of 3
	Support by		
Protocol Element	S	UA O/R	Comments/References
message	O	O/M	
parameters	M	M/M	
delivery-time	O	O/M	
delivery-envelope	O	O/M	See P3 OtherMessage DeliveryFields
data	M	M/M	
mixed-mode	O	O/O	
bilaterally-defined	O	O/O	
nationally-defined	O	O/O	
externally-defined	O	O/M	
parameters	M	M/M	
data	M	M/M	
GeneralTextBodyPart	O	*	

Notes

1 The ability to generate the maximum size subject is not required.

2 May only be included if specifically requested by the originator.

3 The ORName should be specified wherever possible.

4 The ability to generate an IPN is optional in the case of an implementation in which a non-receipt condition cannot occur and receipt notification is not supported (see table 5).

5 The ability to generate non-receipt-fields is optional in the case of an implementation in which a non-receipt condition cannot occur (see note 4).

6 Only the IA5 repertoire has to be supported for an ia5-text body part on reception.

7 The definition of these body parts is for further study in CCITT and ISO.

8 Only the IA5 subset of the T.61 character repertoire need be generated. All T.61 characters should be supported on reception.

A.3 MTS Access Protocol (P3)

NOTE - The support classifications for the IPM UA, MS and MTA below indicate the minimum level of support required by implementations conforming to these Agreements, and should not be misconstrued as a redefinition of any of the MHS application contexts.

Table 36 - Classification of the P3 Protocol Elements

MTS Access Protocol (P3)					Part 1 of 12
	Support by:	IPM UA	MS	MTA	
Protocol Element	S	O/R	O/R	O/R	Comments/References
Operations					
MTSBind	M	M/M	M/M	M/M	MTSBind
MTSUnbind	M	M/M	M/M	M/M	
MSSE					
message-submission	M	M/-	M/M	-/M	MessageSubmission
probe-submission	M	O/-	M/M	-/M	ProbeSubmission
cancel-deferred-delivery	M	O/-	M/M	-/M	CancelDeferredDelivery
submission-control	M	-/M	M/M	O/-	SubmissionControl
MDSE					
message-delivery	M	-/M	M/M	M/-	MessageDelivery
report-delivery	M	-/M	M/M	M/-	ReportDelivery
delivery-control	M	O/-	O/-	-/M	DeliveryControl
MASE					
register	M	O/-	M/M	-/M	Register
change-credentials					
(MTS to MTSuser)	M	-/M	M/M	O/-	ChangeCredentials
(MTSuser to MTS)	M	O/-	M/M	-/M	ChangeCredentials
Note - A Message Store must pass through all MSSE and MASE operations unaltered.					

Table 36 - Classification of the P3 Protocol Elements (continued)

MTS Access Protocol (P3)					Part 2 of 12
	Support by:	IPM UA	MS	MTA	
Protocol Element	S	O/R	O/R	O/R	Comments/References
Arguments/Results					
MTSBind					MTS to MTS User
ARGUMENT					
initiator-name	M	-/M	-/M	M/-	
MTS-user	-	-/-	-/-	-/-	
MTA	O	-/O	-/M	M/-	
isMessageStore	-	-/-	-/-	-/-	
messages-waiting	O	-/O	-/O	O/-	
initiator-credentials	M	-/M	-/M	M/-	
simple	O	-/M	-/M	M/-	
strong	O	-/O	-/O	O/-	
security-context	O	-/O	-/O	O/-	1-256
RESULT					
responder-name	M	M/-	M/-	-/M	
MTS-user	O	M/-	M/-	-/M	
MTA	-	-/-	-/-	-/-	
ismessagestore	O	M/-	M/-	-/M	
messages-waiting	-	-/-	-/-	-/-	
responder-credentials	M	M/-	M/-	-/M	
simple	O	M/-	M/-	-/M	
strong	O	O/-	O/-	-/O	
MTSBind					MTS User to MTS
ARGUMENT					
initiator-name	M	M/-	M/-	-/M	
mTS-user	O	M/-	M/-	-/M	
mTA	-	-/-	-/-	-/-	
isMessageStore	O	M/M	M/-	-/M	
messages-waiting	-	-/-	-/-	-/-	
initiator-credentials	M	M/-	M/-	-/M	
simple	O	M/-	M/-	-/M	
strong	O	O/-	O/-	-/O	
security-context	O	O/-	O/-	-/O	1-256
RESULT					
responder-name	M	-/M	-/M	M/-	
mTS-user	-	-/-	-/-	-/-	
mTA	O	-/M	-/M	M/-	
isMessageStore	-	-/-	-/-	-/-	
messages-waiting	O	-/O	-/O	O/-	
responder-credentials	M	-/M	-/M	M/-	
simple	O	-/M	-/M	M/-	
strong	O	-/O	-/O	O/-	

Table 36 - Classification of the P3 Protocol Elements (continued)

MTS Access Protocol (P3)					Part 3 of 12
	Support by:	IPM UA	MS	MTA	
Protocol Element	S	O/R	O/R	O/R	Comments/References
MessageSubmission					
ARGUMENT					
envelope	M	M/-	M/-	-/M	MessageSubmission Envelope
content	M	M/-	M/-	-/M	
RESULT					
message-submission-identifier	M	-/M	-/M	M/-	See P1 MTSIdentifier
message-submission-time	M	-/M	-/M	M/-	
content-identifier	O	-/M	-/M	M/-	
extensions	O	-/O	-/O	O/-	
originating-MTA-certificate	O	-/O	-/O	O/-	
proof-of-submission	O	-/O	-/O	O/-	
ProbeSubmission					
ARGUMENT					
envelope	M	M/-	M/-	-/M	ProbeSubmission Envelope
RESULT					
probe-submission-identifier	M	-/M	-/M	M/-	See P1 MTSIdentifier
probe-submission-time	M	-/M	-/M	M/-	
content-identifier	O	-/M	-/M	M/-	
CancelDeferredDelivery					
ARGUMENT					
message-submission-identifier	M	M/-	M/-	-/M	See P1 MTSIdentifier
SubmissionControl					
ARGUMENT					
controls	M	-/M	-/M	M/-	See Note 1
restrict	O	-/M	-/M	O/-	
permissible-operations	O	-/M	-/M	O/-	
permissible-maximum-content-length	O	-/M	-/M	O/-	
permissible-lowest-priority	O	-/M	-/M	O/-	
permissible-security-context	O	-/O	-/O	O/-	
RESULT					
waiting	M	M/-	M/-	-/M	See Note 2
waiting-operations	O	O/-	O/-	-/M	0-16
waiting-messages	O	O/-	O/-	-/M	
waiting-content-types	O	O/-	O/-	-/M	0-1024
waiting-encoded-information-types	O	O/-	O/-	-/M	See P1 Encoded InformationTypes

Table 36 - Classification of the P3 Protocol Elements (continued)

MTS Access Protocol (P3)					Part 4 of 12
	Support by:	IPM UA	MS	MTA	
Protocol Element	S	O/R	O/R	O/R	Comments/References
MessageDelivery					
ARGUMENT					
envelope	M	-/M	-/M	M/-	MessageDeliveryEnvelope
content	M	-/M	-/M	M/-	
RESULT					
recipient-certificate	O	O/-	O/-	-/O	
proof-of-delivery	O	O/-	O/-	-/O	
ReportDelivery					
ARGUMENT					
envelope	M	-/M	-/M	M/-	ReportDeliveryEnvelope
returned-content	O	-/M	-/M	O/-	
DeliveryControl					
ARGUMENT					
controls	M	M/-	M/-	-/M	See Note 3
restrict	O	O/-	O/-	-/M	
permissible-operations	O	O/-	O/-	-/M	
permissible-maximum-content-length	O	O/-	O/-	-/M	
permissible-lowest-priority	O	O/-	O/-	-/M	
permissible-content-types	O	O/-	O/-	-/M	
permissible-encoded-information-types	O	O/-	O/-	-/M	See P1 Encoded InformationTypes
permissible-security-context	O	O/-	O/-	-/O	
RESULT					
waiting	M	-/M	-/M	M/-	See Note 4
waiting-operations	O	-/M	-/M	O/-	
waiting-messages	O	-/M	-/M	O/-	
waiting-content-types	O	-/M	-/M	O/-	
waiting-encoded-information-types	O	-/M	-/M	O/-	See P1 Encoded InformationTypes
Register					See Note 5
ARGUMENT					
user-name	O	O/-	O/-	-/O	See X.411, 8.4.1.1.1.1
user-address	O	O/-	O/-	-/O	
deliverable-encoded-information-types	O	O/-	M/-	-/M	See P1 Encoded InformationTypes
deliverable-maximum-content-length	O	O/-	M/-	-/M	
default-delivery-controls	O	O/-	O/-	-/M	
restrict	O	O/-	O/-	-/M	

Table 36 - Classification of the P3 Protocol Elements (continued)

MTS Access Protocol (P3)					Part 5 of 12
		Support by: IPM			
Protocol Element	S	UA O/R	MS O/R	MTA O/R	Comments/References
permissible-operations	O	O/-	O/-	-/M	
permissible-maximum-content-length	O	O/-	O/-	-/M	
permissible-lowest-priority	O	O/-	O/-	-/M	
permissible-content-types	O	O/-	O/-	-/M	1-1024
permissible-encoded-information-types	O	O/-	O/-	-/M	See P1 Encoded InformationTypes
deliverable-content-types	O	O/-	M/-	-/M	1-1024
labels-and-redirections	O	O/-	O/-	-/O	1-256
user-security-label	O	O/-	O/-	-/O	
recipient-assigned-alternate-recipient	O	O/-	O/-	-/O	
ChangeCredentials					MTS to MTSuser
ARGUMENT					
old-credentials	M	-/M	-/M	M/-	Note 8
simple	O	-/M	-/M	O/-	
strong	O	-/O	-/O	O/-	
new-credentials	M	-/M	-/M	M/-	Note 8
simple	O	-/M	-/M	O/-	
strong	O	-/O	-/O	O/-	
ChangeCredentials					MTSuser to MTS
ARGUMENT					
old-credentials	M	M/-	M/-	-/M	Note 8
simple	O	O/-	O/-	-/M	
strong	O	O/-	O/-	-/O	
new-credentials	M	M/-	M/-	-/M	Note 8
simple	O	O/-	O/-	-/M	
strong	O	O/-	O/-	-/O	
MessageSubmissionEnvelope					See Note 6
originator-name	M	M/-	M/-	-/M	See ORName
original-encoded-information-types	O	M/-	M/-	-/M	See P1 Encoded InformationTypes
content-type	M	M/-	M/-	-/M	
built-in	O	O/-	M/-	-/M	
external	O	O/-	M/-	-/M	
content-identifier	O	O/-	M/-	-/M	1-16
priority	O	M/-	M/-	-/M	All values
per-message-indicators	O	M/-	M/-	-/M	
disclosure-of-recipients	O	O/-	M/-	-/M	

Table 36 - Classification of the P3 Protocol Elements (continued)

MTS Access Protocol (P3)					Part 6 of 12
		Support by: IPM			
Protocol Element	S	UA O/R	MS O/R	MTA O/R	Comments/References
implicit-conversion-prohibited	O	M/-	M/-	-/M	
alternate-recipient-allowed	O	M/-	M/-	-/M	
content-return-request	O	O/-	M/-	-/M	
deferred-delivery-time	O	M/-	M/-	-/M	
extensions	O	M/-	M/-	-/M	
recipient-reassignment-prohibited	O	O/-	M/-	-/M	
dl-expansion-prohibited	O	M/-	M/-	-/M	
conversion-with-loss-prohibited	O	O/-	M/-	-/M	
latest-delivery-time	O	O/-	M/-	-/M	
originator-return-address	O	O/-	M/-	-/M	
originator-certificate	O	O/-	O/-	-/O	
content-confidentiality-algorithm-identifier	O	O/-	O/-	-/O	
message-origin-authentication-check	O	O/-	O/-	-/O	
message-security-label	O	O/-	O/-	-/O	
proof-of-submission-request	O	O/-	O/-	-/O	
content-correlator	O	O/-	M/-	-/M	
forwarding-request	O	O/-	M/-	-/M	MS Abstract Service only
PerRecipientMessageSubmission Fields	M	M/-	M/-	-/M	1-32767
recipient-name	M	M/-	M/-	-/M	See ORName
originator-report-request	M	M/-	M/-	-/M	
explicit-conversion	O	O/-	M/-	-/M	
extensions	O	M/-	M/-	-/M	
originator-requested-alternate-recipient	O	O/-	O/-	-/O	
requested-delivery-method	O	M/-	M/-	-/M	Note 9
physical-forwarding-prohibited	O	O/-	M/-	-/M	
physical-forwarding-address-request	O	O/-	O/-	-/O	
physical-delivery-modes	O	O/-	O/-	-/O	
registered-mail-type	O	O/-	O/-	-/O	
recipient-number-for-advice	O	O/-	O/-	-/O	
physical-rendition-attributes	O	O/-	O/-	-/O	
physical-delivery-report-request	O	O/-	O/-	-/O	
message-token	O	O/-	O/-	-/O	
content-integrity-check	O	O/-	O/-	-/O	
proof-of-delivery-request	O	O/-	O/-	-/O	

Table 36 - Classification of the P3 Protocol Elements (continued)

MTS Access Protocol (P3)					Part 7 of 12
	Support by:	IPM UA	MS	MTA	
Protocol Element	S	O/R	O/R	O/R	Comments/References
ProbeSubmissionEnvelope					See Note 6
originator-name	M	M/-	M/-	-/M	See ORName
original-encoded-information-types	O	M/-	M/-	-/M	See P1 Encoded InformationTypes
content-type	M	M/-	M/-	-/M	
built-in	O	O/-	M/-	-/M	0-32767
external	O	O/-	M/-	-/M	
content-identifier	O	O/-	M/-	-/M	1-16
content-length	O	M/-	M/-	-/M	1-'7FFFFFF'H
per-message-indicators	O	M/-	M/-	-/M	
implicit-conversion-prohibited	O	M/-	M/-	-/M	
alternate-recipient-allowed	O	O/-	M/-	-/M	
extensions	O	M/-	M/-	-/M	
recipient-reassignment-prohibited	O	O/-	M/-	-/M	
dl-expansion-prohibited	O	M/-	M/-	-/M	
conversion-with-loss-prohibited	O	O/-	M/-	-/M	
originator-certificate	O	O/-	O/-	-/O	
message-security-label	O	O/-	O/-	-/O	
content-correlator	O	O/-	M/-	-/M	
probe-origin-authentication-check	O	O/-	O/-	-/O	
PerRecipientProbeSubmissionFields	M	M/-	M/-	-/M	1-32767
recipient-name	M	M/-	M/-	-/M	See ORName
originator-report-request	M	M/-	M/-	-/M	
explicit-conversion	O	O/-	M/-	-/M	0-256
extensions	O	M/-	M/-	-/M	
originator-requested-alternate-recipient	O	O/-	O/-	-/O	
requested-delivery-method	O	M/-	M/-	-/M	0-256, Note 9
physical-rendition-attributes	O	O/-	M/-	-/M	
MessageDeliveryEnvelope					See Note 7
message-delivery-identifier	M	-/M	-/M	M/-	See P1 MTSIdentifier
message-delivery-time	M	-/M	-/M	M/-	
other-fields	M	-/M	-/M	M/-	
content-type	M	-/M	-/M	M/-	
built-in	O	-/M	-/M	M/-	0-32767
external	O	-/M	-/M	M/-	
originator-name	M	-/M	-/M	M/-	See ORName

Table 36 - Classification of the P3 Protocol Elements (continued)

MTS Access Protocol (P3)					Part 8 of 12
	Support by:	IPM UA	MS	MTA	
Protocol Element	S	O/R	O/R	O/R	Comments/References
original-encoded-information-types	O	-/M	-/M	M/-	See P1 Encoded InformationTypes
priority	O	-/M	-/M	M/-	All values
delivery-flags	O	-/M	-/M	M/-	
implicit-conversion-prohibited	O	-/M	-/M	M/-	
other-recipient-names	O	-/M	-/M	M/-	See ORName
this-recipient-name	M	-/M	-/M	M/-	See ORName
originally-intended-recipient-name	O	-/M	-/M	M/-	See ORName
converted-encoded-information-types	O	-/M	-/M	M/-	See P1 Encoded InformationTypes
message-submission-time	M	-/M	-/M	M/-	
content-identifier	O	-/M	-/M	M/-	1-16
extensions	O	-/M	-/M	M/-	
conversion-with-loss-prohibited	O	-/M	-/M	M/-	
requested-delivery-method	O	-/M	-/M	M/-	Note 9
physical-forwarding-prohibited	O	-/-	-/-	M/-	
physical-forwarding-address-request	O	-/-	-/-	M/-	
physical-delivery-modes	O	-/-	-/-	M/-	0-16
registered-mail-type	O	-/-	-/-	M/-	0-256
recipient-number-for-advice	O	-/-	-/-	M/-	1-32
physical-rendition-attributes	O	-/-	-/-	M/-	
physical-delivery-report-request	O	-/-	-/-	M/-	0-256
originator-return-address	O	-/-	-/-	M/-	
originator-certificate	O	-/O	-/O	O/-	
message-token	O	-/O	-/O	O/-	
content-confidentiality-algorithm-identifier	O	-/O	-/O	O/-	
content-integrity-check	O	-/O	-/O	O/-	
message-origin-authentication-check	O	-/O	-/O	O/-	
message-security-label	O	-/O	-/O	O/-	
proof-of-delivery-request	O	-/O	-/O	O/-	
redirection-history	O	-/M	-/M	M/-	1-512
dl-expansion-history	O	-/M	-/M	M/-	1-512

Table 36 - Classification of the P3 Protocol Elements (continued)

MTS Access Protocol (P3)					Part 9 of 12
	Support by:	IPM UA	MS	MTA	
Protocol Element	S	O/R	O/R	O/R	Comments/References
ReportDeliveryEnvelope					See Note 7
subject-submission-identifier	M	-/M	-/M	M/-	See P1 MTSIdentifier
content-identifier	O	-/M	-/M	M/-	
content-type	O	-/M	-/M	M/-	
built-in	O	-/M	-/M	M/-	0-32767
external	O	-/M	-/M	M/-	
original-encoded-information-types	O	-/M	-/M	M/-	See P1 Encoded InformationTypes
extensions	O	-/M	-/M	M/-	
message-security-label	O	-/O	-/O	O/-	
content-correlator	O	-/M	-/M	M/-	
originator-and-DL-expansion-history	O	-/M	-/M	M/-	See P1 OriginatorAndDL ExpansionHistory
reporting-DL-name	O	-/M	-/M	M/-	
reporting-MTA-certificate	O	-/O	-/O	O/-	
report-origin-authentication-check	O	-/O	-/O	O/-	
PerRecipientReportDelivery-Fields	M	-/M	-/M	M/-	1-32767
actual-recipient-name	M	-/M	-/M	M/-	See ORName
report	M	-/M	-/M	M/-	
delivery	O	-/M	-/M	M/-	
message-delivery-time	M	-/M	-/M	M/-	
type-of-MTS-user	O	-/M	-/M	M/-	
non-delivery	O	-/M	-/M	M/-	
non-delivery-reason-code	M	-/M	-/M	M/-	
non-delivery-diagnostic-code	O	-/M	-/M	M/-	
converted-encoded-information-types	O	-/M	-/M	M/-	See P1 Encoded InformationTypes
originally-intended-recipient-name	O	-/M	-/M	M/-	See ORName
supplementary-information	O	-/M	-/M	M/-	1-256
extensions	O	-/M	-/M	M/-	
redirection-history	O	-/M	-/M	M/-	See P1 Redirection History, 1-512
physical-forwarding-address	O	-/M	-/M	M/-	
recipient-certificate	O	-/O	-/O	O/-	
proof-of-delivery	O	-/O	-/O	O/-	
ORName					MTS User to MTS
standard-attributes					
country-name	O	M/-	M/-	-/	CountryName
administration-domain-name	O	M/-	M/-	-/M	DomainName
network-address	O	O/-	O/-	-/M	
terminal-identifier	O	O/-	O/-	-/M	

Table 36 - Classification of the P3 Protocol Elements (continued)

MTS Access Protocol (P3)					Part 10 of 12
	Support by:	IPM UA	MS	MTA	
Protocol Element	S	O/R	O/R	O/R	Comments/References
private-domain-name	O	M/-	M/-	-/M	DomainName
organization-name	O	M/-	M/-	-/M	
numeric-user-identifier	O	O/-	O/-	-/M	
personal-name	O	M/-	M/-	-/M	
surname	M	M/-	M/-	-/M	
given-name	O	M/-	M/-	-/M	
initials	O	M/-	M/-	-/M	
generation-qualifier	O	M/-	M/-	-/M	
organizational-unit-names	O	M/-	M/-	-/M	
OrganizationUnitName	M	M/-	M/-	-/M	
domain-defined-attributes	O	M/-	M/-	-/M	
DomainDefinedAttribute	M	M/-	M/-	-/M	
type	M	M/-	M/-	-/M	
value	M	M/-	M/-	-/M	
extension-attributes	O	M/-	M/-	-/M	ExtensionAttribute
common-name	O	M/-	M/-	-/M	
teletex-common-name	O	O/-	O/-	-/M	
teletex-organization-name	O	M/-	O/-	-/M	
teletex-personal-name	O	M/-	O/-	-/M	
teletex-organizational-unit-names	O	M/-	O/-	-/M	
teletex-domain-defined-attributes	O	M/-	O/-	-/M	
pds-name	O	O/-	O/-	-/M	
physical-delivery-country-name	O	O/-	O/-	-/M	
postal-code	O	O/-	O/-	-/M	
physical-delivery-office-name	O	O/-	O/-	-/M	
physical-delivery-office-number	O	O/-	O/-	-/M	
extension-OR-address-components	O	O/-	O/-	-/M	
physical-delivery-personal-name	O	O/-	O/-	-/M	
physical-delivery-organization-name	O	O/-	O/-	-/M	
extension-physical-delivery-address-components	O	O/-	O/-	-/M	
unformatted-postal-address	O	O/-	O/-	-/M	
street-address	O	O/-	O/-	-/M	
post-office-box-address	O	O/-	O/-	-/M	
poste-restante-address	O	O/-	O/-	-/M	
unique-postal-name	O	O/-	O/-	-/M	
local-postal-attributes	O	O/-	O/-	-/M	
extended-network-address	O	O/-	O/-	-/M	
terminal-type	O	O/-	O/-	-/M	
ORName					MTS to MTS User
standard-attributes					
country-name	O	-/M	-/M	M/-	CountryName

Table 35 - Classification of the P3 Protocol Elements (continued)

MTS Access Protocol (P3)					Part 11 of 12
		Support by: IPM			
Protocol Element	S	UA O/R	MS O/R	MTA O/R	Comments/References
administration-domain-name	O	-/M	-/M	M/-	DomainName
network-address	O	-/M	-/M	M/-	
terminal-identifier	O	-/M	-/M	M/-	
private-domain-name	O	-/M	-/M	M/-	DomainName
organization-name	O	-/M	-/M	M/-	
numeric-user-identifier	O	-/M	-/M	M/-	
personal-name	O	-/M	-/M	M/-	
surname	M	-/M	-/M	M/-	
given-name	O	-/M	-/M	M/-	
initials	O	-/M	-/M	M/-	
generation-qualifier	O	-/M	-/M	M/-	
organizational-unit-names	O	-/M	-/M	M/-	
OrganizationUnitName	M	-/M	-/M	M/-	
domain-defined-attributes	O	-/M	-/M	M/-	
DomainDefinedAttribute	M	-/M	-/M	M/-	
type	M	-/M	-/M	M/-	
value	M	-/M	-/M	M/-	
extension-attributes	O	-/M	-/M	M/-	ExtensionAttribute
common-name	O	-/M	-/M	M/-	
teletex-common-name	O	-/M	-/M	M/-	
teletex-organization-name	O	-/M	-/M	M/-	
teletex-personal-name	O	-/M	-/M	M/-	
teletex-organizational-unit-names	O	-/M	-/M	M/-	
teletex-domain-defined-attributes	O	-/M	-/M	M/-	
pds-name	O	-/O	-/M	M/-	
physical-delivery-country-name	O	-/O	-/M	M/-	
postal-code	O	-/O	-/M	M/-	
physical-delivery-office-name	O	-/O	-/M	M/-	
physical-delivery-office-number	O	-/O	-/M	M/-	
extension-OR-address-components	O	-/O	-/M	M/-	
physical-delivery-personal-name	O	-/O	-/M	M/-	
physical-delivery-organization-name	O	-/O	-/M	M/-	
extension-physical-delivery-address-components	O	-/O	-/M	M/-	
unformatted-postal-address	O	-/O	-/M	M/-	
street-address	O	-/O	-/M	M/-	
post-office-box-address	O	-/O	-/M	M/-	
poste-restante-address	O	-/O	-/M	M/-	
unique-postal-name	O	-/O	-/M	M/-	
local-postal-attributes	O	-/O	-/M	M/-	
extended-network-address	O	-/O	-/M	M/-	
terminal-type	O	-/O	-/M	M/-	

Table 36 - Classification of the P3 Protocol Elements (concluded)

MTS Access Protocol (P3)	Part 12 of 12

Notes

1 The MTS-user may interpret any restriction as simply withhold 'all' submissions.

2 No explicit action needs to be taken by the MTA.

3 The MTA may interpret any restriction as simply withhold 'all' deliveries.

4 No explicit action needs to be taken by the MTS-user.

5 The Register operation may be performed locally (see X.411). Although not required for the UA for conformance, it is considered to be a useful service and support is recommended.

6 The action to be taken by a submitting MTA is as defined in X.411 (ISO 10021-4). In the absence of any specific processing requirements for a particular element in a submission envelope, the action to be taken is simply the faithful mapping of such element to the corresponding element of the appropriate transfer envelope.

7 The action to be taken by a delivering MTA is as defined in X.41 (ISO 10021-4). In the absence of any specific processing requirements for a particular element in a delivery envelope, the action to be taken is simply the creation of such element from the corresponding element of the appropriate transfer envelope.

8 At least one of simple and/or strong must be specified.

9 Applies to ORNames containing Directory Names and/or ORAddresses See Recommendation X.411, section 8.2.1.1.1.14.

A.4 MS Access Protocol (P7)

Table 37 - Classification of the P7 Protocol Elements

MS Access Protocol (P7)				Part 1 of 6
	Support by:	IPM UA	MS	
Protocol Element	S	O/R	O/R	Comments/References
Operations				
MSBind	M	M/-	-/M	MSBind
MSUnbind	M	M/-	-/M	
MSSE				
message-submission	M	M/-	-/M	See P3 MessageSubmission
probe-submission	M	O/-	-/M	See P3 ProbeSubmission
cancel-deferred-delivery	M	O/-	-/M	See P3 CancelDeferred Delivery
submission-control	M	-/M	M/-	See P3 SubmissionControl
MASE				
register	M	O/-	-/M	See P3 Register
change-credentials (MS to UA)	M	-/M	M/-	See P3 ChangeCredentials
change-credentials (UA to MS)	M	O/-	-/M	See P3 ChangeCredentials
MRSE				
summarize	M	M/-	-/M	Summarize
list	M	M/-	-/M	List
fetch	M	M/-	-/M	Fetch
delete	M	M/-	-/M	Delete
register-ms	M	O/-	-/M	Register-MS
alert	M	-/O	O/-	Alert
Arguments/Results				
MSBind				
ARGUMENT				
MSBindArgument	M	M/-	-/M	
initiator-name	M	M/-	-/M	
initiator-credentials	M	M/-	-/M	
simple	O	M/-	-/M	
strong	O	O/-	-/O	
security-context	O	O/-	-/O	
fetch-restrictions	O	O/-	-/M	
allowed-content-types	O	O/-	-/M	
allowed-EITs	O	O/-	-/M	
maximum-content-length	O	O/-	-/M	
MS-configuration-request	O	O/-	-/M	

Table 37 - Classification of the P7 Protocol Elements (continued)

MS Access Protocol (P7)				Part 2 of 6
	Support by:	IPM UA	MS	
Protocol Element	S	O/R	O/R	Comments/References
RESULT				
MSBindResult	M	-/M	M/-	
responder-credentials	M	-/M	M/-	
simple	O	-/M	M/-	
strong	O	-/O	O/-	
available-auto-actions	O	-/M	M/-	1-16
available-attribute-types	O	-/M	M/-	1-1024
alert-indication	O	-/M	O/-	
content-types-supported	O	-/M	M/-	
Summarize				
ARGUMENT				
SummarizeArgument	M	M/-	-/M	
information-base-type	O	O/-	-/M	InformationBase
selector	M	M/-	-/M	Selector
summary-requests	O	O/-	-/M	1-16
RESULT				
SummarizeResult	M	-/M	M/-	
next	O	-/M	M/-	
count	M	-/M	M/-	1-'7FFFFFFF'H
span	O	-/M	M/-	
lowest	M	-/M	M/-	
highest	M	-/M	M/-	
summaries	O	-/M	M/-	1-16
absent	O	-/M	M/-	1-'7FFFFFFF'H
present	O	-/M	M/-	1-32767
type	M	-/M	M/-	
value	M	-/M	M/-	
count	M	-/M	M/-	
List				
ARGUMENT				
ListArgument	M	M/-	-/M	
information-base-type	O	O/-	-/M	InformationBase
selector	M	M/-	-/M	Selector
requested-attributes	O	M/-	-/M	AttributeSelection
RESULT				
ListResult	M	-/M	M/-	
next	O	-/M	M/-	
requested	O	-/M	M/-	EntryInformation, 0-'7FFFFFFF'H

Table 37 - Classification of the P7 Protocol Elements (continued)

MS Access Protocol (P7)				Part 3 of 6
	Support by:	IPM UA	MS	
Protocol Element	S	O/R	O/R	Comments/References
Fetch				
ARGUMENT				
FetchArgument	M	M/–	–/M	
information-base-type	O	O/–	–/M	InformationBase
item	M	M/–	–/M	
search	O	M/–	–/M	Selector
precise	O	M/–	–/M	
requested-attributes	O	M/–	–/M	AttributeSelection
RESULT				
FetchResult	M	–/M	M/–	
entry-information	O	–/M	M/–	EntryInformation
list	O	–/M	M/–	0–'7FFFFFFF'H
next	O	–/M	M/–	
Delete				
ARGUMENT				
DeleteArgument	M	M/–	–/M	
information-base-type	O	O/–	–/O	InformationBase
items	M	M/–	–/M	
selector	O	M/–	–/M	Selector
sequence-numbers	O	M/–	–/M	1–'7FFFFFFF'H
RESULT				
DeleteResult	M	–/M	M/–	
Register-MS				
ARGUMENT				
Register-MSArgument	M	M/–	–/M	
auto-action-registrations	O	O/–	–/O	1–1024
type	M	M/–	–/M	
registration-identifier	O	M/–	–/M	
registration-parameter	M	M/–	–/M	See auto action registration parameters
auto-action-deregistrations	O	O/–	–/O	1–1024
type	M	M/–	–/M	
registration-identifier	O	M/–	–/M	
list-attribute-defaults	O	M/–	–/M	1–1024
fetch-attribute-defaults	O	M/–	–/M	1–1024
change-credentials	O	M/–	–/M	Note 1
old-credentials	M	M/–	–/M	
new-credentials	M	M/–	–/M	
user-security-labels	O	O/–	–/O	1–256
RESULT				
Register-MSResult	M	–/M	M/–	

Table 37 - Classification of the P7 Protocol Elements (continued)

MS Access Protocol (P7)				Part 4 of 6
	Support by:	IPM UA	MS	
Protocol Element	S	O/R	O/R	Comments/References
Alert				
ARGUMENT				
AlertArgument	M	–/M	M/–	
alert-registration-identifier	M	–/M	M/–	
new-entry	O	–/M	M/–	EntryInformation
RESULT				
AlertResult	O	M/–	–/M	
Auto Action Registration Parameters				
AutoForwardRegistrationParameter				
filter	O	O/–	–/M	Filter
auto-forward-arguments	M	M/–	–/M	
originator-name	M	M/–	–/M	
content-identifier	O	O/–	–/M	
priority	O	O/–	–/M	
per-message-indicators	O	O/–	–/M	See P3
deferred-delivery-time	O	O/–	–/M	
extensions	O	O/–	–/M	See P3
per-recipient-fields	M	M/–	–/M	
recipient-name	M	M/–	–/M	
originator-report-request	M	M/–	–/M	
explicit-conversion	O	O/–	–/M	
extensions	O	O/–	–/M	See P3
delete-after-auto-forwarding	O	O/–	–/M	
other-parameters	O	O/–	–/M	See Note 2
auto-forwarding-comment	O	O/–	–/M	
cover-note	O	O/–	–/M	
this-ipm-prefix	O	O/–	–/M	
AutoAlertRegistrationParameter				
filter	O	O/–	–/M	Filter
alert-addresses	O	O/–	–/O	
address	M	M/–	–/M	
alert-qualifier	O	O/–	–/O	
requested-attributes	O	O/–	–/M	AttributeSelection

Table 37 - Classification of the P7 Protocol Elements (continued)

MS Access Protocol (P7)				Part 5 of 6
	Support by:	IPM UA	MS	
Protocol Element	S	O/R	O/R	Comments/References
Common Data Types				
AttributeSelection				
type	M	M/-	-/M	
from	O	O/-	-/M	1-32767
count	O	O/-	-/M	1-32767
AttributeValueAssertion				
type	M	M/-	-/M	
value	M	M/-	-/M	
EntryInformation				
sequence-number	M	-/M	M/-	
attributes	O	-/M	M/-	1-1024
type	M	-/M	M/-	
values	M	-/M	M/-	
Filter				
item	O	M/-	-/M	FilterItem
and	O	O/-	-/O	1-32
or	O	O/-	-/O	1-32
not	O	O/-	-/O	
FilterItem				
equality	O	M/-	-/M	AttributeValueAssertion (Support is O if Orname)
substrings	O	O/-	-/O	
type	M	M/-	-/M	
strings	M	M/-	-/M	
initial	O	O/-	-/M	
any	O	O/-	-/M	
final	O	O/-	-/M	
greater-or-equal	O	O/-	-/M	AttributeValueAssertion
less-or-equal	O	O/-	-/M	AttributeValueAssertion
present	O	O/-	-/M	
approximate-match	O	O/-	-/O	
InformationBase				
stored-messages	O	M/-	-/M	
inlog	O	O/-	-/O	
outlog	O	O/-	-/O	

Table 37 - Classification of the P7 Protocol Elements (concluded)

MS Access Protocol (P7)				Part 6 of 6
	Support by:	IPM UA	MS	
Protocol Element	S	O/R	O/R	Comments/References
Range				
sequence-number-range	O	O/–	–/M	
from	O	O/–	–/M	
to	O	O/–	–/M	
creation-time-range	O	O/–	–/M	
from	O	O/–	–/M	
to	O	O/–	–/M	
Selector				
child-entries	O	O/–	–/M	
range	O	O/–	–/M	Range
filter	O	O/–	–/M	Filter
limit	O	O/–	–/M	
override	O	O/–	–/M	

Notes
1 At least one of simple and/or strong must be specified.
2 The specified syntax of other-parameters is for IPMS use only – see X.413 section 12.1 and X.420 section 19.4.

A.5 Classification of the P1 Protocol Elements for Security Classes

The protocol element classifications used in tables 38 and 39 should be viewed as a delta to the lower security class or, if there is no lower security class, to the kernel as classified in table 34. Thus, table 38 shows the additional support required in P1 to conform to security class S1. Table 39 indicates the additional support required to support security class S2 (above and beyond that for security class S1).

NOTES

1 There are no additional classifications for security class S0.

2 The addition of mandatory content confidentiality does not affect the P1 protocol.

Table 38 - Conformance Classification of the P1 Protocol Elements for Security Class S1

MTS Transfer Protocol (P1) for Security Class S1				Part 1 of 2
	MT Kernel Static Support by MTS Class			
Protocol Element	B/C O/R	A O/R	Dyn	Comments/References
MTABind				
ARGUMENT				
<SET>				
initiator-credentials			M	
simple	O/O	O/O	X	
strong	M/M	M/M	M	
bind-token	M/M	M/M	M	
certificate	O/O	O/O		
security-context	M/M	M/M	M	
RESULT				
<SET>				
responder-credentials			M	
simple	O/O	O/O	X	
strong	M/M	M/M	M	
bind-token	M/M	M/M	M	
certificate	O/O	O/O		
MessageTransferEnvelope				
extensions				
message-security-label	M/M	M/M	M	

Table 38 - Conformance Classification of the P1 Protocol Elements for Security Class S1
(concluded)

MTS Transfer Protocol (P1) for Security Class S1				Part 2 of 2
	MT Kernel Static Support by MTS Class			
Protocol Element	B/C O/R	A O/R	Dyn	Comments/References
ReportTransferEnvelope				
extensions				
message-security-label	M/M	M/M		See Note 2
per-recipient-fields				
extensions				
message-token	O/O	O/O	M	
asymmetric-token				
signed-data				
message-security-label	M/M	M/M	M	See Note 2
encrypted-data				
message-security-label	M/M	M/M		See Note 2
bind-token				
asymmetric-token				See Note 1
signature-algorithm-identifier	M/M	M/M	M	
name	M/M	M/M	M	
time	M/M	M/M	M	
signed-data	M/M	M/M	M	
encryption-algorithm-identifier	M/M	M/M		
encrypted-data	M/M	M/M		
message-security-label	M/M	M/M		
content-integrity-key	M/M	M/M		
message-security-label	M/M	M/M	M	See Note 2
security-policy-identifier	M/M	M/M	M	

Notes
1 In line with the CCITT MHS Implementors' Guide, the asymmetric token can be used by symmetric and asymmetric techniques as identified by the algorithm identifier.
2 The message security label may appear in any or all of the indicated locations in the envelope. However the Security context service applies only to the label in the "extensions" and/or token signed-data as defined by the security policy in force. Labels in th token encrypted data have only end-to-end (UA-to-UA) significance.

Table 39 - Conformance Classification of the P1 Protocol Elements for Security Class S2

MTS Transfer Protocol (P1) for Security Class S2				Part 1 of 2
	MT Kernel Static Support by MTS Class			
Protocol Element	B/C O/R	A O/R	Dyn	Comments/References
MessageTransferEnvelope				
extension				
originator-certificate	M/M	M/M		
certificate	M/M	M/M		
certification-path	M/M	M/M		
message-origin-authentication-check	M/M	M/M	M	
algorithm-identifier	M/M	M/M		
content	M/M	M/M		
content-identifier	M/M	M/M		
message-security-label	M/M	M/M		
ProbeTransferEnvelope				
extensions				
originator-certificate	M/M	M/M		
certificate	M/M	M/M		
certification-path	M/M	M/M		
probe-origin-authentication-check	M/M	M/M	M	
algorithm-identifier	M/M	M/M		
content-identifier	M/M	M/M		
message-security-label	M/M	M/M		
ReportTransferEnvelope				
extensions				
reporting-MTA-certificate	M/M	M/M		
certificate	M/M	M/M		
certification-path	M/M	M/M		
report-origin-authentication-check	M/M	M/M	M	
algorithm-identifier	M/M	M/M		
content-identifier	M/M	M/M		
message-security-label	M/M	M/M		
per-recipient	M/M	M/M		
actual-recipient-name	M/M	M/M		
originally-intended-recipient-name	O/O	O/O		
delivery	O/O	O/O		
message-delivery-time	M/M	M/M		
type-of-MTS-user	M/M	M/M		
recipient-certificate	M/M	M/M		
proof-of-delivery	M/M	M/M		
non-delivery	O/O	O/O		
non-delivery-reason-code	M/M	M/M		
non-delivery-diagnostic-code	O/O	O/O		

Table 39 - Conformance Classification of the P1 Protocol Elements for Security Class S2
(concluded)

MTS Transfer Protocol (P1) for Security Class S2				Part 2 of 2
	MT Kernel Static Support by MTS Class			
Protocol Element	B/C O/R	A O/R	Dyn	Comments/References
Certificate				
version	M/M	M/M		
serialNumber	M/M	M/M		
signature	M/M	M/M		
algorithm	M/M	M/M		
parameters	O/O	O/O		
issuer	M/M	M/M		
validity	M/M	M/M		
notBefore	M/M	M/M		
notAfter	M/M	M/M		
subject	M/M	M/M		
subjectPublicKeyInfo	M/M	M/M		
algorithm	M/M	M/M		
subjectPublicKey	M/M	M/M		

A.6 Classification of the P3 Protocol Elements for Security Classes

The protocol element classifications in tables 40, 41, and 42 should be viewed as a delta to the lower security class or, if there is no lower security class, to the kernel as classified in table 36. Thus, table 40 shows the additional support required in P3 to conform to security class S0. Table 41 indicates the additional support required to support security class S1 (above and beyond that for security class S0). Table 42 indicates the additional support required to support security class S2 (above and beyond that for security class S1).

NOTE - There are no dynamic conformance classifications required by security class S0 (table 40).

Table 40 - Conformance Classification of the P3 Protocol Elements for Security Class S0

MTS Access Protocol (P3) for Security Class S0					Part 1 of 2
	Static Support by: IPM				
Protocol Element	UA O/R	MS O/R	MTA O/R	Dyn	Comments/References
MessageDelivery					
RESULT					
proof-of-delivery	M/-	M/-	-/O		
MessageSubmissionEnvelope					
PerRecipientMessageSubmission Fields					
extensions					
message-token	M/-	M/-	-/O		
asymmetric-token	M/-	M/-	-/O		
signature-algorithm-identifier	M/-	M/-	-/O		
name	M/-	M/-	-/O		
time	M/-	M/-	-/O		
signed-data	M/-	M/-	-/O		
content-confidentiality-algorithm-identifier	O/-	O/-	-/O		
content-integrity-check	M/-	M/-	-/O		See Note 1
message-security-label	O/-	O/-	-/O		
proof-of-delivery-request	M/-	M/-	-/O		See Note 1
message-sequence-number	O/-	O/-	-/O		
encryption-algorithm-identifier	O/-	O/-	-/O		
encrypted-data	M/-	M/-	-/O		
content-confidentiality-key	O/-	O/-	-/O		
content-integrity-check	M/-	M/-	-/O		See Note 1
message-security-label	O/-	O/-	-/O		
content-integrity-key	O/-	O/-	-/O		
message-sequence-number	O/-	O/-	-/O		
content-integrity-check	M/-	M/-	-/O		See Note 1
proof-of-delivery-request	M/-	M/-	-/O		See Note 1

Table 40 - Conformance Classification of the P3 Protocol Elements for Security Class S0
(concluded)

MTS Access Protocol (P3) for Security Class S0					Part 2 of 2
	Static Support by: IPM				
Protocol Element	UA O/R	MS O/R	MTA O/R	Dyn	Comments/References
MessageDeliveryEnvelope					
other-fields					
extensions					
message-token	-/M	-/M	O/-		
asymmetric-token	-/M	-/M	O/-		
signature-algorithm-identifier	-/M	-/M	O/-		
name	-/M	-/M	O/-		
time	-/M	-/M	O/-		
signed-data	-/M	-/M	O/-		
content-confidentiality-algorithm-identifier	-/O	-/O	O/-		
content-integrity-check	-/M	-/M	O/-		See Note 1
message-security-label	-/O	-/O	O/-		
proof-of-delivery-request	-/M	-/M	O/-		See Note 1
message-sequence-number	-/O	-/O	O/-		
encryption-algorithm-identifier	-/O	-/O	O/-		
encrypted-data	-/M	-/M	O/-		
content-confidentiality-key	-/O	-/O	O/-		
content-integrity-check	-/M	-/M	O/-		See Note 1
message-security-label	-/O	-/O	O/-		
content-integrity-key	-/O	-/O	O/-		
message-sequence-number	-/O	-/O	O/-		
content-integrity-check	-/M	-/M	O/-		See Note 1
proof-of-delivery-request	-/M	-/M	O/-		See Note 1
ReportDeliveryEnvelope					
PerRecipientReportDelivery-Fields					
extensions					
proof-of-delivery	-/M	-/O	O/-		

Notes
1 Implementations shall generate no more that one instance of these identically-named protocol elements in a single message.

Table 41 - Conformance Classification of the P3 Protocol Elements for Security Class S1

MTS Access Protocol (P3) for Security Class S1					Part 1 of 3
	Static Support by: IPM				
Protocol Element	UA O/R	MS O/R	MTA O/R	Dyn	Comments/References
MTSBind					MTS to MTS User
ARGUMENT					
initiator-credentials				M	
simple	-/O	-/O	O/-	X	
strong	-/M	-/M	M/-	M	
bind-token	-/M	-/M	M/-	M	
certificate	-/O	-/O	O/-		
security-context	-/M	-/M	M/-	M	
RESULT					
responder-credentials				M	
simple	O/-	O/-	-/O	X	
strong	M/-	M/-	-/M	M	
bind-token	M/-	M/-	-/M	M	
certificate	O/-	O/-	-/O		
MTSBind					MTS User to MTS
ARGUMENT					
initiator-credentials				M	
simple	O/-	O/-	-/O	X	
strong	M/-	M/-	-/M	M	
bind-token	M/-	M/-	-/M	M	
certificate	O/-	O/-	-/O		
security-context	M/-	M/-	-/M	M	
RESULT					
responder-credentials				M	
simple	-/O	-/O	O/-	X	
strong	-/M	-/M	M/-	M	
bind-token	-/M	-/M	M/-	M	
certificate	-/O	-/O	O/-		
SubmissionControl	-/M	M/M	M/-		
ARGUMENT					
controls					
permissible-security-context	-/M	-/M	M/-		
DeliveryControl	M/-	M/-	-/M		
ARGUMENT					
controls					
permissible-security-context	M/-	M/-	-/M		
Register					
ARGUMENT					
user-name	M/-	M/-	-/M		
labels-and-redirections					
user-security-label	M/-	M/-	-/M		

Table 41 - Conformance Classification of the P3 Protocol Elements for Security Class S1
(continued)

MTS Access Protocol (P3) for Security Class S1					Part 2 of 3
	Static Support by: IPM				
Protocol Element	UA O/R	MS O/R	MTA O/R	Dyn	Comments/References
ChangeCredentials					MTS to MTSuser
ARGUMENT					
old-credentials				M	
simple	-/O	-/O	O/-	X	
strong	-/M	-/M	M/-	M	
bind-token	-/M	-/M	M/-	M	
certificate	-/O	-/O	O/-		
new-credentials				M	
simple	-/O	-/O	O/-	X	
strong	-/M	-/M	M/-	M	
bind-token	-/M	-/M	M/-	M	
certificate	-/O	-/O	O/-		
ChangeCredentials					MTSuser to MTS
ARGUMENT					
old-credentials				M	
simple	O/-	O/-	-/O	X	
strong	M/-	M/-	-/M	M	
bind-token	M/-	M/-	-/M	M	
certificate	O/-	O/-	-/O		
new-credentials				M	
simple	O/-	O/-	-/O	X	
strong	M/-	M/-	-/M	M	
bind-token	M/-	M/-	-/M	M	
certificate	O/-	O/-	-/O		
MessageSubmissionEnvelope					
extensions					
message-token	M/-	M/-	-/M		
signed-data					
message-security-label	M/-	M/-	-/M		See Note 1
security-policy-identifier	M/-	M/-	-/M	M	
encrypted-data					
message-security-label	O/-	O/-	-/O		
content-integrity-check	M/-	M/-	-/M	M	
message-security-label	M/-	M/-	-/M		See Note 1
security-policy-identifier	M/-	M/-	-/M	M	
MessageDeliveryEnvelope					
extensions					
message-security-label	-/M	-/M	M/-		See Note 1
security-policy-identifier	-/M	-/M	M/-	M	
message-token	-/M	-/M	M/-		
signed-data					
message-security-label	-/O	-/O	O/-		See Note 1
encrypted-data					
message-security-label	-/O	-/O	O/-		See Note 1

Table 41 - Conformance Classification of the P3 Protocol Elements for Security Class S1
(concluded)

MTS Access Protocol (P3) for Security Class S1					Part 3 of 3
	Static Support by: IPM				
Protocol Element	UA O/R	MS O/R	MTA O/R	Dyn	Comments/References
ReportDeliveryEnvelope					
extensions					
message-security-label	-/M	-/M	M/-	M	See Note 1
bind-token					
asymmetric-token					
signature-algorithm-identifier	-/M	-/M	M/-	M	
name	-/M	-/M	M/-	M	
time	-/M	-/M	M/-	M	
signed-data	-/M	-/M	M/-	M	
encryption-algorithm-identifier	-/M	-/M	M/-		
encrypted-data	-/M	-/M	M/-		
message-security-label	-/M	-/M	M/-		
content-integrity-key	-/M	-/M	M/-		

Notes
1 The message-security-label may appear in any or all of the indicated locations in the envelope. However, the security labelling context services apply only to the label in the "extensions" field. Labels in th message token have only end-to-end (UA-to-UA) significance.

Table 42 - Conformance Classification of the P3 Protocol Elements for Security Class S2

MTS Access Protocol (P3) for Security Class S2					Part 1 of 2
	Static Support by: IPM				
Protocol Element	UA O/R	MS O/R	MTA O/R	Dyn	Comments/References
MessageSubmission					
RESULT					
extensions					
originating-MTA-certificate	-/M	-/O	M/-		
certificate	-/-	-/O	-/-		
certification-path	-/-	-/O	-/-		
proof-of-submission	-/M	-/O	M/-		
MessageDelivery					
RESULT					
recipient-certificate	M/-	M/-	-/O		
certificate	M/-	M/-	-/M		
certification-path	M/-	M/-	-/M		
MessageSubmissionEnvelope					
extensions					
originator-certificate	M/-	O/-	-/M		

certificate	-/-	-/O	-/-		
certification-path	-/-	-/O	-/-		
message-origin-authentication-check	M/-	O/-	-/M	M	
algorithm-identifier	M/-	M/-	-/M		
content	M/-	M/-	-/M		
content-identifier	M/-	M/-	-/M		
message-security-label	M/-	M/-	-/M		
proof-of-submission-request	M/-	O/-	-/M		
ProbeSubmissionEnvelope					
extensions					
originator-certificate	M/-	O/-	-/M		
certificate	-/-	-/O	-/-		
certification-path	-/-	-/O	-/-		
probe-origin-authentication-check	M/-	O/-	-/M	M	
algorithm-identifier	M/-	M/-	-/M		
content-identifier	M/-	M/-	-/M		
message-security-label	M/-	M/-	-/M		

Table 42 - Conformance Classification of the P3 Protocol Elements for Security Class S2
(concluded)

MTS Access Protocol (P3) for Security Class S2					Part 2 of 2
	Static Support by: IPM				
Protocol Element	UA O/R	MS O/R	MTA O/R	Dyn	Comments/References
MessageDeliveryEnvelope					
extensions					
originator-certificate	-/M	-/M	M/-		
certificate	-/M	-/M	M/-		
certification-path	-/M	-/M	M/-		
message-origin-authentication-check	-/M	-/M	M/-	M	
algorithm-identifier	-/M	-/M	M/-		
content	-/M	-/M	M/-		
content-identifier	-/M	-/M	M/-		
message-security-label	-/M	-/M	M/-		
ReportDeliveryEnvelope					
extensions					
reporting-MTA-certificate	-/M	-/O	M/-		
certificate	-/-	-/O	-/-		
certification-path	-/-	-/O	-/-		
report-origin-authentication-check	-/M	-/O	M/-	M	
PerRecipientReportDeliveryFields					
extensions					
recipient-certificate	-/M	-/M	O/-		
certificate	-/M	-/M	M/-		
certification-path	-/M	-/M	M/-		
Certificate					
version	-/M	-/M	M/-		

serialNumber	-/M	-/M	M/-		
signature	-/M	-/M	M/-		
algorithm	-/M	-/M	M/-		
parameters	-/O	-/O	O/-		
issuer	-/M	-/M	M/-		
validity	-/M	-/M	M/-		
notBefore	-/M	-/M	M/-		
notAfter	-/M	-/M	M/-		
subject	-/M	-/M	M/-		
subjectPublicKeyInfo	-/M	-/M	M/-		
algorithm	-/M	-/M	M/-		
subjectPublicKey	-/M	-/M	M/-		

Table 43 presents the classification delta to classification tables 40, 41, and 42, for the addition of mandatory content confidentiality in the static conformance classification.

NOTE - There are no dynamic conformance classification required by the addition of content confidentiality.

Table 43 - Conformance Classification of the P3 Protocol Elements for Security Classes S0a, S1a, or S2a

MTS Access Protocol (P3) for Security Classes S0a, S1a, S2a					Part 1 of 1
	Static Support by: IPM				
Protocol Element	UA O/R	MS O/R	MTA O/R	Dyn	Comments/References
MessageSubmissionEnvelope					
extensions					
content-confidentiality-algorithm-identifier	M/-	O/-	-/O		
message-token					
asymmetric-token					
signed-data	M/-	-/-	-/-		
content-confidentiality-algorithm-identifier	M/-	-/-	-/-		
encrypted-data					
content-confidentiality-key	M/-	-/-	-/-		
MessageDeliveryEnvelope					
extensions					
message-token	-/M	-/M	O/-		
asymmetric-token					
signed-data	-/M	-/M	-/-		
content-confidentiality-algorithm-identifier	-/M	-/M	-/-		
encrypted-data					
content-confidentiality-key	-/M	-/M	-/-		
content-confidentiality-algorithm-identifier	-/M	-/M	O/-		

Notes
1 Implementors shall generate no more than one instance of these identically named protocol elements in a single message.

A.7 Classification of the P7 Protocol Elements for Security Classes

The protocol element classifications in table 44 should be viewed as a delta to the lower security class or, if there is no lower security class, to the kernel as classified in table 37. Thus, table 44 shows the additional support required in P7 to conform to security class S1.

NOTES

1 There are no additional classifications for security classes S0 and S2.

2 The addition of mandatory content confidentiality does not affect the P7 protocol.

Table 44 - Conformance Classification of the P7 Protocol Elements for Security Class S1

MS Access Protocol (P7) for Security Class S1				Part 1 of 1
	Static Support by: IPM			
Protocol Element	UA O/R	MS O/R	Dyn	Comments/References
MSBind				
ARGUMENT				
initiator-credentials			M	
simple	O/-	-/O	X	
strong	M/-	-/M	M	
bind-token	M/-	-/M	M	
certificate	O/-	-/O		
security-context	M/-	-/M	M	
RESULT				
responder-credentials			M	
simple	-/O	O/-	X	
strong	-/M	M/-	M	
bind-token	-/M	M/-	M	
certificate	-/O	O/-		
Register-MS				
ARGUMENT				
Register-MSArgument				
changeCredentials			M	
old-credentials	M/-	-/M	M	
simple	O/-	-/O	M	
strong	M/-	-/M	X	
bind-token	M/-	-/M	M	
certificate	O/-	-/O		
new-credentials	M/-	-/M	M	
simple	O/-	-/O	X	
strong	M/-	-/M	M	
bind-token	M/-	-/M	M	
certificate	O/-	-/O		
user-security-labels	M/-	-/M	M	
message-security-label				
security-policy-identifier	M/-	-/M	M	
security-classification	M/-	-/M		
privacy	O/-	-/O		
security-categories	M/-	-/M		

A.8 Message Store General Attribute Support

Table 45 - Classification of the Message Store General Attributes

Message Store General Attribute Support					Part 1 of 2
Support by:		IPM UA	Bas MS	IPM MS	
Attribute	S	Rec	Org	Org	Comments/References
child-sequence-numbers	M	M	M	M	
content	M	M	M	M	
content-confidentiality-algorithm-identifier	O	O	O	O	
content-correlator	O	O	O	M	
content-identifier	O	O	O	M	
content-integrity-check	O	O	O	O	
content-length	O	O	O	M	
content-returned	O	O	O	M	
content-type	M	M	M	M	
conversion-with-loss-prohibited	O	O	O	M	
converted-eits	O	O	O	M	
creation-time	M	M	M	M	
delivered-eits	O	O	O	M	
delivery-flags	O	O	O	M	
dl-expansion-history	O	O	O	M	
entry-status	M	M	M	M	
entry-type	M	M	M	M	
intended-recipient-name	O	O	O	M	
message-delivery-envelope	M	M	M	M	
message-delivery-identifier	O	O	O	M	
message-delivery-time	O	O	O	M	
message-origin-authentication-check	O	O	O	O	
message-security-label	O	O	O	O	
message-submission-time	O	O	O	M	
message-token	O	O	O	O	
original-eits	O	O	O	M	
originator-certificate	O	O	O	O	
originator-name	O	O	O	M	
other-recipient-names	O	O	O	M	
parent-sequence-number	M	M	M	M	
per-recipient-report-delivery-fields	M	M	M	M	
priority	O	O	O	M	
proof-of-delivery-request	O	O	O	O	
redirection-history	O	O	O	M	
report-delivery-envelope	M	M	M	M	
reporting-dl-name	O	O	O	O	
reporting-mta-certificate	O	O	O	O	

Table 45 - Classification of the Message Store General Attributes (concluded)

Message Store General Attribute Support					Part 2 of 2
Attribute	S	IPM UA Rec	Bas MS Org	IPM MS Org	Comments/References
report-origin-authentication-check	O	O	O	O	
security-classification	O	O	O	O	
sequence-number	M	M	M	M	
subject-submission-identifier	M	M	M	M	
this-recipient-name	O	O	O	M	

Note - Enhanced MS support for optional Functional Groups is for further study. Attributes which are relevant to these areas are currently specified as Unsupported.

A.9 Classification of the IPM MS General Attributes for Security Classes

The classification of the attributes in table 46 is a delta to the MS General Attributes classified in table 38. Table 46 indicates the additional attributes that must be supported in the IPM MS for each of the security classes. There is no support required for security attributes in the basic MS.

Table 46 - IPM MS Security Attribute Support

	Security Class					
Attribute	S0	S0a	S1	S1a	S2	S2a
content-confidentiality-algorithm-identifier	O	M	O	M	O	M
content-integrity-check	M	M	M	M	M	M
message-security-label	O	O	M	M	M	M
message-origin-authentication-check	M	M	M	M	M	M
message-token	M	M	M	M	M	M
origination-certificate	O	O	O	O	M	M
proof-of-delivery	M	M	M	M	M	M
reporting-mta-certificate	O	O	O	O	M	M
report-origin-authentication-check	O	O	O	O	M	M
security-classification	O	O	M	M	M	M

A.10 Message Store IPM Attribute Support

This clause is to be read in accordance with Annex C of X.420 (1988).

Table 47 - Classification of the Message Store IPM Attributes

Message Store IPM Attribute Support				Part 1 of 2
	Support by:	IPM UA	IPM MS	
Attribute	S	Rec	Org	Comments/References
Summary Attributes:				
ipm-entry-type	O	O	M	
ipm-synopsis	O	O	M	
Heading Attributes:				
authorizing-users	O	O	M	
auto-forwarded	O	O	M	
blind-copy-recipients	O	O	M	
copy-recipients	O	O	M	
expiry-time	O	O	M	
heading	M	M	M	
importance	O	O	M	
incomplete-copy	O	O	O	
languages	O	O	M	
nrn-requestors	O	O	M	
obsoleted-ipms	O	O	M	
originator	O	O	M	
primary-recipients	O	O	M	
related-ipms	O	O	M	
replied-to-ipm	O	O	M	
reply-recipients	O	O	M	
reply-requestors	O	O	M	
reply-time	O	O	M	
rn-requestors	O	O	M	
sensitivity	O	O	M	
subject	O	O	M	
this-ipm	M	M	M	
Body Attributes:				
bilaterally-defined-body-parts	O	O	O	
body	M	M	M	
encrypted-body-parts	O	O	O	
encrypted-data	O	O	O	
encrypted-parameters	O	O	O	
extended-body-part-types	O	O	O	

Table 47 - Classification of the Message Store IPM Attributes (concluded)

Message Store IPM Attribute Support				Part 2 of 2
	Support by:	IPM UA	IPM MS	
Attribute	S	Rec	Org	Comments/References
g3-facsimile-body-parts	O	O	O	
g3-facsimile-data	O	O	O	
g3-facsimile-parameters	O	O	O	
g4-class1-body-parts	O	O	O	
ia5-text-body-parts	O	O	M	
ia5-text-data	O	O	O	
ia5-text-parameters	O	O	O	
message-body-parts	O	O	M	
message-data	O	O	O	
message-parameters	O	O	O	
mixed-mode-body-parts	O	O	O	
nationally-defined-body-parts	O	O	O	
teletex-body-parts	O	O	O	
teletex-data	O	O	O	
teletex-parameters	O	O	O	
videotex-body-parts	O	O	O	
videotex-data	O	O	O	
videotex-parameters	O	O	O	
voice-body-parts	O	O	O	
voice-data	O	O	O	
voice-parameters	O	O	O	
Notification Attributes:				
acknowledgment-mode	O	O	M	
auto-forward-comment	O	O	M	
conversion-eits	O	O	M	
discard-reason	O	O	M	
ipm-preferred-recipient	O	O	M	
ipn-originator	O	O	M	
non-receipt-reason	O	O	M	
receipt-time	O	O	M	
returned-ipm	O	O	O	
subject-ipm	M	M	M	
suppl-receipt-info	O	O	O	

A.11 EDI Messaging Service Protocol (Pedi)

See Working Document.

A.12 Message Store EDIMS Attribute Support

See Working Document.

Annex B (normative)

List of ASN.1 Object Identifiers

B.1 Content Types

See Working Document.

B.2 Body Part Types

See Working Document.

B.3 Security Classes

The ASN.1 expressed in figure 15 defines the security Object Identifiers specified by these Implementation Agreements. These are the same as defined in the EWOS/ETSI A/3311 profile.

```
id-mhs-security              OBJECT IDENTIFIER ::= { iso (1)
  identified-organization (3) ewos (16) eg (2) mhs (4) security (4) }

id-policy-id                 OBJECT IDENTIFIER ::= { id-mhs-security 1 }
id-category-id               OBJECT IDENTIFIER ::= { id-mhs-security 2 }

-- Security Policy Object Identifiers --

security-class-0             OBJECT IDENTIFIER ::= { id-policy-id 0 }
security-class-0a            OBJECT IDENTIFIER ::= { id-policy-id 0 1 }
security-class-1             OBJECT IDENTIFIER ::= { id-policy-id 1 }
security-class-1a            OBJECT IDENTIFIER ::= { id-policy-id 1 1 }
security-class-2             OBJECT IDENTIFIER ::= { id-policy-id 2 }
security-class-2a            OBJECT IDENTIFIER ::= { id-policy-id 2 1 }

-- Security Category Object Identifiers --

private-id                   OBJECT IDENTIFIER ::= { id-category-id 0 }
confidence-id                OBJECT IDENTIFIER ::= { id-category-id 1 }
commercial-in-confidence-id  OBJECT IDENTIFIER ::= { id-category-id 2 }
management-in-confidence-id  OBJECT IDENTIFIER ::= { id-category-id 3 }
personal-in-confidence-id    OBJECT IDENTIFIER ::= { id-category-id 4 }
```

Figure 15 - Security Object Identifiers

Annex C (informative)

Interpretation of Elements of Service

The objective of this clause is to provide clarification, where required, on the functionality of Elements of Service where the MHS standards are unclear or ambiguous. It is not the intent of this clause to define how information should be made available or presented to an MHS user, nor is it intended to define how individual vendors should design their products.

The following MHS Elements of Service require further text to be added to their definitions to represent the proposed implementation of these Elements of Service for conformance to this Agreement. Elements of Service which are not referenced in this clause are as defined in the MHS base standards.

Reply Request Indication: The reply-recipients and the reply-time may be specified without any explicit reply being requested. This may be interpreted by the recipient as an implicit reply request.

NOTE - For an auto-forwarded message, an explicit or implicit reply request may not be meaningful.

Forwarded IP-message Indication: The following use of the original encoded information type in the context of forwarded messages is clarified:

a) The encoded information types of the message being forwarded should be reflected in the new original encoded information types being generated;

b) if forwarding a privately defined body part (see figure 4), the originator of the forwarding message shall set the original encoded information types in the P1 envelope to Underfined for that body part.

Annex D (informative)

Recommended Practices

This clause provides guidelines on areas not addressed by the base standards. These guidelines have been produced in order to promote awareness of interim solution to problems as agree by members of the OIW X.400 SIG. However implementors of these recommended practices should note that it is not necessary to follow the recommended practices when claiming conformance to these agreements.

Implementors should also note that future standardization by CCITT and ISO/IEC on area covered by this clause may result in different solutions to those proposed in this clause.

D.1 Printable String

There are existing mail systems that include a small set of non-Printable String characters in their identifiers. For these systems to communicate with MHS systems, either for pass-through service or delivery to MHS users, gateways will be employed to encode these special characters into a sequence of Printable String characters. This conversion should be performed by the gateway according to a common scheme and before insertion in Domain Defined Attributes, which are intended to carry electronic mail identifiers. MHS UAs may also perform such conversions.

It is recommended that the following symmetrical encoding and decoding algorithm for non-Printable String characters be employed. The encoding algorithm maps an ASCII representation to a PrintableString representation. Any non-printable string characters not specified in table 50 are covered by the category "other".

Table 50 - Printable String to ASCII Mapping

ASCII Character	Printable String Character
% (percent)	(p)
@ (at sign)	(a)
! (exclamation)	(b)
" (quote mark)	(q)
_ (underline)	(u)
((left paren.)	(l)
) (right paren.)	(r)
other	(3DIGIT)

where 3DIGIT has the range 000 to 377 and is interpreted as the octal encoding of an ASCII character.

To encode an ASCII representation to a PrintableString, table 50 and the algorithm in figure 16 should be used.

```
IF current character is in the encoding set THEN
  encode the character according to table 50
ELSE
  write the current character;
continue reading;
```

Figure 16 - ASCII to PrintableString Algorithm.

To decode a PrintableString representation to an ASCII representation, table 50 and the algorithm in figure 17 should be used.

```
IF current character is not "(" THEN
  write character
ELSE
  {
  look ahead appropriate characters;
  IF composite characters are in table 50 THEN
     decode per table 50
  ELSE
  write current character;
  }
continue reading;
```

Figure 17 - PrintableString to ASCII Algorithm.

The actual technique employed depends on the algorithm used. Algorithms are assumed to be bilaterally agreed or registered by a registration authority. However, the algorithm-identifier must be unique and unambiguously define the algorithm.

It is recommended that a conforming ASN.1 BIT STRING is normally used to contain the encrypted data (as generated by use for the ENCRYPTED macro), thereby ensuring insertion of padding zero bits which may be necessary for correct operation of certain algorithms. Alternatively, the implementation should take such action explicitly.

It is recommended that, in the absence of any requirement for support of other specific algorithms, implementations shall as a default support algorithms identified in CCITT X.509 (ISO/IEC 9594-8). It is also strongly recommended that implementations are capable of using any encryption-based technique on a "plug-in" or modular basis.

In the case of verification of SIGNATUREs (e.g., proof of delivery, MOAC, POAC, or ROAC), implementations should assume that all relevant data present in the subject message, probe, or report has been included in the signature.

D.1.1Implementation Considerations

D.1.1.1Peer Entity Authentication

Peer entity authentication is provided using the strong authentication mechanisms on the various Bind operations, using either asymmetric or symmetric techniques. The key management information necessary for symmetric peer entity authentication is outside the scope of these Implementation Agreements.

D.1.1.2Confidentiality

Connection confidentiality is provided using the underlying OSI layers and is outside the scope of these Implementation Agreements. Mechanisms to support connection confidentiality are subject to bilateral agreement between peers (i.e., connection confidentiality may even be achieved by trusting the connection to the peer OSI entity).

Content Confidentiality may be achieved by either symmetric or asymmetric encryption techniques. It should be noted that use of asymmetric techniques precludes submission of messages to multiple recipients.

D.1.1.3Integrity

Connection Integrity is provided using the underlying OSI layers and is outside the scope of these Implementation Agreements. Mechanisms to support Connection Integrity are subject to bilateral agreement between peers. It should be noted that the integrity of a connection can be increased by use of RTSE.

Content Integrity is achieved by computing a content integrity check as a function of the entire message content. When symmetric techniques are used to compute the content integrity check a secret key is required. This content integrity key may be confidentially sent to the message recipient using the message argument confidentiality security element in the message token (i.e., there may be other keys or parts of the key not sent by the originator with the message, but the key management of such external keys is outside the scope of these Implementation Agreements). It should be noted that placing the content integrity check in the encrypted data of the message token will provide additional protection against masquerade threats.

NOTE - Content Integrity can also provide integrity of receipt and non-receipt notifications (IPNs) and can assist in the provision of "non-repudiation of receipt" since non-repudiation of delivery may be insufficient where delivery is to a Message Store.

D.1.1.4Message Origin Authentication

End-to-end (i.e., UA to UA) Message Origin Authentication is automatically provided by content integrity. Security classes S2 and S2a provide additional protection (i.e., of the integrity of the label) by requiring support of origin authentication checks within the MTS.

D.1.1.5Non-Repudiation

If asymmetric techniques are used for content integrity it can also provide non-repudiation of origin (UA to UA) depending on the level of trust placed in the certificate. If symmetric techniques are used, content integrity can also provide non-repudiation of origin, but only by using a trusted notary to validate the content integrity and provide trusted key management facilities. A degree of non-repudiation can be provided by the use of trusted accountability services.

NOTE - It is assumed that an originating UA will ensure that delivery notification is requested when proof of delivery is requested.

D.1.1.6Secure Access Management

Secure Access Management can be implemented by a combination of Multi-Level Security (MLS) functionality by assurance of the various MHS components to support such functionality. MLS

functionality is supported in the base standards by the use of security labels, security context and the security token and can be applied in a hierarchical and/or role manner depending on the policy requirements of a domain.

MLS assurance will generally also require other (COMPUSEC) measures and is outside the scope of the base standards and these Implementation Agreements. Reference should be made to the appropriate security authority and any applicable security evaluation criteria (e.g., U. S. DoD Orange Book, UK - Netherlands - Germany - France draft Evaluation Criteria).

D.1.1.7Implications for the Use of Distribution Lists

An MTA performing distribution list expansion must create all the per-recipients fields for the members of the distribution list. It may either generate a new token for each DL member (i.e., using the recipient name of that DL member) or alternatively it may copy the same token (i.e., containing the recipient name of the DL itself) into the per-recipient fields for each DL member. In the former case, the content-integrity-check should not be changed if it is to be used to provide message origin authentication. Also in such case, the DL expansion point must have at least the same security class as the originator and must have trusted functionality. The choice of which approach to use will therefore need to be determined in accordance with the security policy which may prohibit the use of distribution lists altogether.

D.1.1.8Implications on Redirection

The Security Functional Group has the effect of either requiring trust in any redirection facilities or prohibiting the use of redirection. If the Redirection facility is to be trusted, it must be subject to the security policy and obey the security labels as defined in the base standards. It is recommended that the token is not altered on redirection (i.e., it will contain the originally-specified recipient name).

D.1.1.9Implications for 1984 Interworking

Interworking between implementations conforming to Security Functional Groups and 1984 systems is not supported. The Double Enveloping technique can be used to traverse an 1984 system.

D.1.1.10Implications for Use of Directory

The X.400 security services use of the directory service does not require a trusted directory because the information that is retrieved is certified and can be validated independently of the directory.

Other threats (e.g., malicious corruption of directory information) may arise from the broader use of the directory, however these are outside of the scope of the X.400 base standard and this Implementors Agreement.

Work continues within CCITT and ISO to improve the security inherent in the Directory standards.

D.1.1.11Implications for Conversion

Implementation of the Security functional group may additionally either require that any conversion facilities are highly trusted to regenerate the appropriate security elements (notably the content integrity check) or prohibit the use of conversion within the MTS altogether. In particular, it should be noted that use of conversion facilities will invalidate any origin authentication based on the original content.

D.1.1.12Accountability

Accountability depends on the identification and authentication of users, then subsequent records being kept on the actions taken by users. Therefore, accountability depends on all the relevant information being properly stored or recorded.

Accountability features provided by domains (or MTAs) are subject to bilateral agreement between domains (or MTAs) and may optionally provide non-repudiation services. Accountability features include pervasive mechanisms such as security logs, audit trails and archives, or they may be mechanisms supported by protocol. Protocols to support accountability will be subject to bilateral agreement.

D.1.1.13Double Enveloping

Double enveloping can be used with each secure messaging security class. For each security class it is an optional extension to the security features which can be used to counter specific vulnerabilities. When double enveloping is used, it shall be applied at the boundary of a domain, and obey the rules of an MTA at management domain boundaries. Figure 20 illustrates the technique.

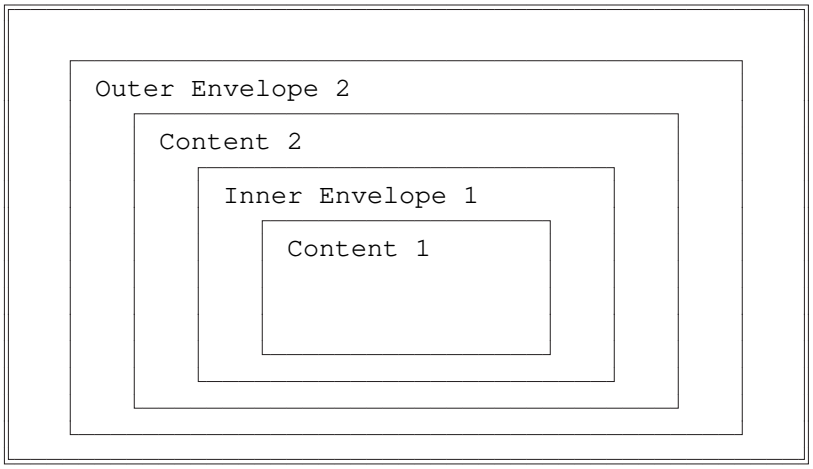

Figure 20 - Double Enveloping Technique.

Address information in envelope 1 and 2 are not necessarily the same.

Trace information in envelope 1 and 2 are not necessarily the same.

The double envelope technique can be used in 1984 and 1988 MTS environments. When used in an

1988 environment, any security class can be applied to the outer envelope. It is recommended that the inner envelope is encrypted. When the double envelope technique is used as a secure relay path via an 1984 domain, any encryption of the content 2 is subject to bilateral agreement.

Trace information is not passed between inner and outer envelopes. It is recommended that trace information on the outer envelope is always archived when the double envelope technique is used.

D.2Security Class S0

D.2.1Rationale

Security class S0 is confined to security functionality operating between MTS-Users on an end-to-end basis. It is designed to minimize the required functionality in the MTS to support submission of elements associated with these services. Security services which must be supported (i.e., must be made available) are those which are considered in any secure messaging environment, i.e.:

a) Content Integrity;

b) Message Origin Authentication (end-to-end);

c) Proof of Delivery.

Other security services, such as Content Confidentiality, may optionally be supported.

D.2.2Technical Implications

The technical implications for security class S0 are:

a) It is necessary to provide mechanisms in a UA which can generate the signed, signature and encrypted macros on message submission;

b) It is necessary to provide mechanisms in a UA which can handle the signed, signature and encrypted macros on message delivery.

D.3Security Class S1

D.3.1Rationale

The S1 security class is a superset of security class S0 and introduces the basic requirement for security functionality not only within the MTS-User but also within the MTS. This security functionality within the MTS is designed to support the enforcement of a security policy within a security domain. As a consequence, S1 enables trusted routing to be implemented.

NOTE - The level of trust in the route will depend on the level of trust in the security label and security context.

D.3.2Technical Implications

The technical implications of security class S1 are:

a) It is necessary to provide mechanisms in a UA which can generate the signed, signature and encrypted macros on message submission.

b) It is necessary to provide mechanisms in a UA which can handle the signed, signature and encrypted macros on message delivery.

c) It is necessary to provide mechanisms in the MTA for registration, change-credentials and bind abstract operations (i.e., signed macro for bind).

d) It is necessary to provide mechanisms in the MS for MS-registration and MS-bind operation (i.e., signed macro for MS-Bind).

e) It is necessary to support message security labelling (the level of assurance is subject to individual security domain requirements).

f) It is necessary that reliable access is always supported.

g) It is necessary for the MTAs to check the existence of the security elements which are classified as "dynamic mandatory".

h) It is necessary to provide a trusted connection between peers to provide adequate confidentiality, integrity and peer entity authentication.

D.4Security Class S2

D.4.1Rationale

Security Class S2 is a superset of Security Class S1. It enhances the facilities of the MTAs in order to check the origination of messages, probes, and reports within the MTS and to provide enhanced integrity checks on the security label while in the MTS. The extra security services provided by this security class can help to provide trusted routing within an MTS.

Additionally, it is possible to provide non-repudiation within an MTS.

D.4.2Technical Implications

The extra security services specified by Security Class S2 use asymmetric techniques exclusively.

The technical implications are as in Security Class S1, plus:

a) It is necessary to provide mechanisms in an MTA and UA that can process the signed macro of certificates;

b) The constraint that the option of supporting Content Confidentiality cannot be allowed when the message origin authentication check (MOAC) is used to provide non-repudiation services. Under this condition Content Confidentiality is not supported. If the MOAC is not used for this purpose, Content Confidentiality can be supported as an optional security service;

c) It is necessary to provide mechanisms in a MTA which can generate and process the signature macro of a message, probe, and report authentication check (MOAC, POAC and ROAC);

d) It is necessary to provide mechanisms in a UA and MTA that can interface with an X.500 directory supporting the Authentication Framework as defined in X.509/ISO 9594-8 or can distrubute public keys by other trusted means which is compliant with X.509;

e) It is necessary to provide a trusted means of generating certificates;

f) It is necessary to provide mechanisms in the MTA which can process a proof of submission request and generate the proof of submission signature;

g) It is necessary to provide a mechanism in an MTA which will generate ROAC signatures with reports;

h) Connection confidentiality is only provided by this security class when the message-origin-authentication-check is computed using clear content to provide non-repudiation of origin security service (i.e., non-repudiation is provided only on the clear content of the message);

i) The irrevocable proof required to provide non-repudiation within the MTS is achieved by the management of asymmetric keys. The explicit definition of asymmetric key management is outside the scope of these Implementors Agreements.

D.5Confidential Security Class Variants (S0a, S1a, and S2a)

D.5.1Rationale

These security class variants are supersets of S0, S1, and S2, adding the requirement for support of end-to-end content confidentiality. The rationale for these variants is to avoid the implementation cost and processing overhead involved in encrypting the entire message content unless there is a definite requirement. It is also possible to protect the encryption techniques and mechanisms (i.e., algorithms, key lengths, key versions, etc.) by Secure Access Management.

D.5.2Technical Implications

The technical implications of the confidential security class variants are the same as those for the corresponding primary security class, plus:

a) It is necessary to provide mechanisms in a UA which can use the encrypted macros to encrypt and decrypt the message content.

Annex E (informative)

Bibliography

E.1ANSI

Procedures for Registering Organization Names in the United States of America, ISSB 843, December 5, 1989.

Procedures for Registering Names in the United States of America, ISSB 840, December 5, 1989. The United States Register is included.