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

Output from the September 1993 Open Systems Environment Implementors' Workshop (OIW)

SIG Chair: **Chris Bonatti, Booz Allen & Hamilton**
SIG Editor: **Rich Ankney, Fischer International**

Foreword

The text in this part contains a set of Message Handling System (MHS) Implementation Agreements intended to serve in lieu of an International Standardized Profile (ISP) for MHS. It is the aim of the OIW X.400 SIG to pursue alignment of this part with the developing ISP. When the ISP is complete, this part will be revised to refer to the ISP, and to only highlight additional practices and North American regional requirements.

Table of Contents

Annex A (normative)

Annex B (normative)

Annex C (informative)

Annex D (informative)

Annex E (informative)

List of Figures

List of Tables

Part 8 Message Handling Systems

0 Introduction

This is an Implementation Agreement developed by the Implementors' 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 the CCITT X.400 (1988) series of Recommendations, the similar (but not identical) ISO MOTIS standard, and Recommendations F.435 and X.435 (1991) (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; and,

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

This Implementation Agreement is designed to encourage 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. These 1988 aspects are described in this Agreement as either incremental enhancements or new functional groups.

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); and,

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).

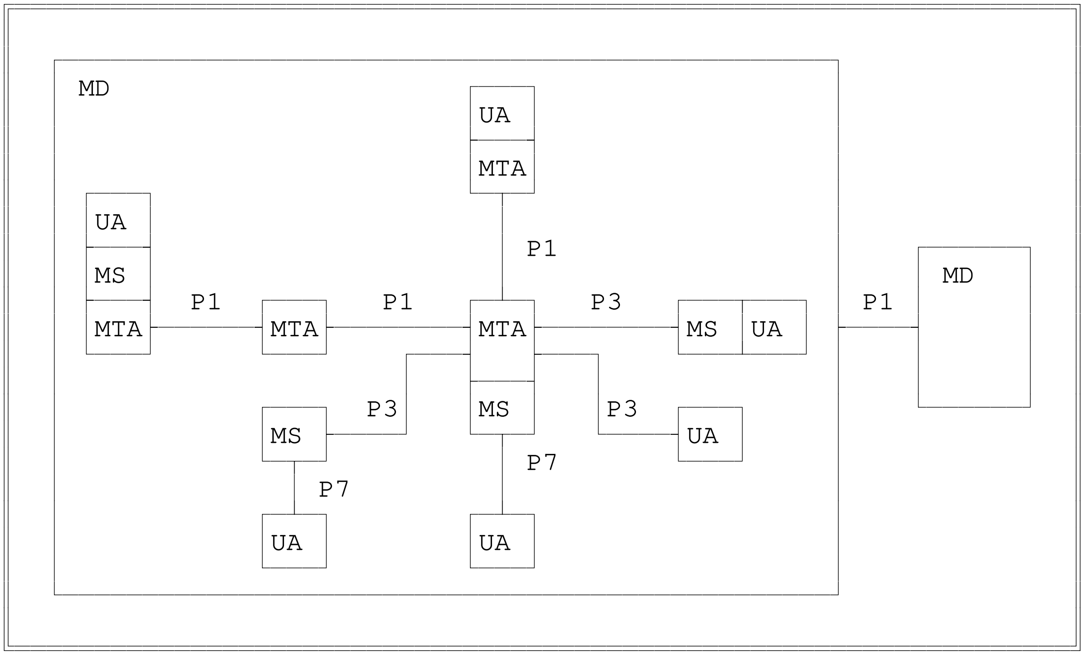

Figure 1 - Scenario definition

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 17.

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 Message Store in clause 6;

c) Remote User Agent support in clause 7;

d) Distribution Lists in clause 8.3;

e) Use of Directory in clause 8.4;

f) Address support for Teletex character sets in clause 8.5;

g) MHS Management in clause 9 (which is for further study);

h) Security in clause 10;

i) The Physical Delivery Access Unit in clause 11.1;

j) Other Access Units in clause 11.2 (which are for further study);

k) Redirection in clause 12 (which is for further study); and,

l) The IPM Service in clause 13;

m) The EDI Messaging Service in clause 14 (which is for further study).

2 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 Recommendation X.435 (1991), *Message Handling Systems, EDI Messaging System, Protocol Specifications*.

CCITT Recommendation F.435 (1991), *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 6.

The initial version of these Stable Implementation Agreements included an Agreement which specified a minimal 1988-based MHS implementation and support for Message Stores and Remote User Agents, and which addresses interworking with 1984-based implementations. This version of the Agreement specifies support for several additional 1988 features. 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 6);

b) Remote UA (see clause 7);

c) Distribution Lists (see clause 8.3);

d) Use of Directory Services (see clause 8.4);

e) Security (see clause 10);

f) Interworking with Physical Delivery systems or Specialized Access (see clause 11); and,

g) Conversion of body parts (see clause 13.6.2).

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); and,

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. Table 1 specifies the support for the basic MT Kernel elements of service and table 2 specifies the support for the optional MT Kernel elements of service.

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; and,

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 clause 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[5,7]	-	-
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~~O	~~M~~O	-
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 8.3).

5 Support of this MT Element of Service does not imply the capability to perform DL expansion (see clause 8.3).

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

7 Support of this EoS has been made mandatory as the default is "allowed". Only the capability to generate the "prohibited" value is required for conformance to the ISP.

5.3 MTS transfer protocol (P1)

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

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 14.10.

5.4 MTS - APDU size

This clause is not intended to constrain the size of PDUs that are transferred across the network, since some body part types and content types (e.g., voice, file transfer, and EDI) may require very large PDUs.

The following agreements govern the size of MTS-APDUs:

a) All MTAEs must support at least one MTS-APDU of at least two megabytes; and,

b) The size of the largest MTS-APDU content supported by a UAE is a local matter.

5.4.1 Number of recipient names

There is no specified bound on the number of recipient-names an implementation must support, other than the 32K-1 specified in the standard (Annex B/X.411).

5.5 1988/84 interworking considerations

An MTA conforming to this Agreement will downgrade 1988 P1 to 1984 P1 when relaying to 1984-based MTAs, as specified in Annex B of X.419 with the following additional requirements:

a) Supplementary Information - will need to be truncated if it exceeds the pragmatic constraint identified in Version 2 of these Agreements (64 octets as opposed to 256 octets in the 1988 MHS standards);

b) ISO DIS 8883 Extensions - An implementation may perform the mapping of ISO DIS 8883 extensions to existing 1988 services when relevant, but is not obliged to. Alternatively, it may discard the extensions or generate a non-delivery report;

c) Internal Trace Information - If the 1984-based MTA does not support Internal Trace Information per clause 7.3.2 of part 7, the following description is not applicable. When a 1988-based MTA supports interworking with a 1984-based MTA that generates Internal Trace Information as per clause 7.3.3 of part 7, the 1988-based MTA must support reception of the Internal Trace Information by converting the Internal Trace Information from the form in clause 7.3.2 of part 7 to the form specified in 1988 X.411, as per the following description. When the 1988-based MTA sends to a 1984 MTA, the 1988-based MTA must apply the conversion to 1984, as described below. The Stable NBS Implementation Agreements X.400 (1984) definition for MTA's Internal Trace Information is different from the X.400 (1988) MTA definition. Consequently, a X.400 (1988) MTA operating in an MD with other MTAs of 1984 vintage, must map the Internal Trace Information to and/or from the 1984 format.

Figures 2 and 3 depict algorithms for mapping between X.400 (1988) Internal Trace element formats and the OIW IA X.400 (1984) Internal Trace element format.

To avoid potential looping within a MD composed of 1984 and 1988 vintage MTAs, MD administrators are strongly advised to name all MTAs (1984 and 1988 vintages) using only the Printable String characters. In X.400 (1988) the MTA-Name is defined to be named using IA5 String characters where in the IAs for X.400 (1984) MTAs, NBS restricted the MTA-Name to be formed using the Printable String character subset of IA5. If the 1988-based MTA Name uses IA5 characters not in the Printable String subset, that Internal Trace Element should be omitted when converting from 1988 to 1984.

```
For each Internal Trace element in the sequence:
DO
  IF MTA-Name is made up of non-Printable String characters:
    Discard this Internal Trace element;
  ELSE
    {  Discard the GlobalDomainIdentifier;
       Copy the MTAname over;
       Within the MTASuppliedInformation:
         Copy the arrival time over;
         Copy the routing action over;
         IF attempted is present
           {  IF it is a domain:
                Discard it;
              IF it is an MTA:
                Copy it to Previous MTAName;
           }
         IF the additional actions are present:
           {  IF the deferred time is present:
                Copy it over;
              IF the other-actions is present:
                Discard it;
           }
    }
END-DO
```

Figure 2 - 1988 to 1984 mapping

```
Find the [APPLICATION 30] entry in the P1 envelope;
FOR each Internal Trace element:
  DO
    Insert the GlobalDomainIdentifier of this MTA;
    Copy the MTAName over;
    Within the MTASuppliedInfo:
      Copy the arrival time;
      IF the deferred time is present:
        copy it to the additional actions field within the
          1988 Internal Trace information;
      IF the routing action is Relayed or Rerouted:
        copy it over;
      IF the routing action is Recipient-reassigned:
        map to Relayed;
      IF the previous MTAName is present:
        copy it to the MTAName in the attempted field;

  END-DO
```

Figure 3 - 1984 to 1988 mapping

NOTE - The 1988 X.419 Recommendation acknowledges that a 1984 system may receive messages containing new distinguished [integer] values that it is not expecting, and that this may result in service irregularities. It is implied that it would be optimal for 1984 systems to accept these unexpected integer values if at all possible. No downgrading should be done for these values when passing affected messages from newer systems to older systems.

6 Message store

6.1 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 4 illustrates the logical relationship of the MS to the UA and MTS.

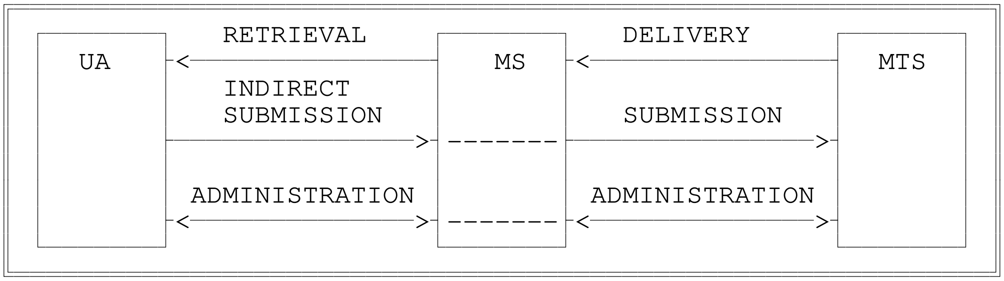

Figure 4 - Message store model

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 7, 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).

6.2 Scope

The scope of the Agreements in this clause is depicted in figure 5, 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.

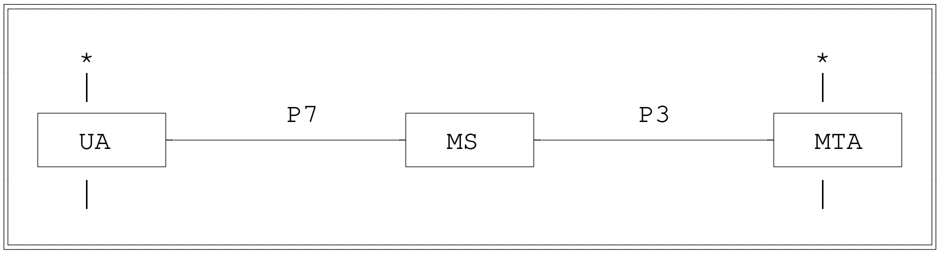

Figure 5 - Scope of message store agreements

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.

6.3 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 4 both for the Message Store itself and for the User Agent.

Table 4 - Message store: elements of service

Element of Service	UA	MS
MS Register	O	M
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

6.4 Attribute types

Requirements for support of the attributes used in the Message Store are detailed in clauses A.8 and A.9.

There are two levels of support for General Attributes in the Message Store.

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 content-specific attributes.

The Enhanced MS supports a larger number of general attributes and is suited to MSs that also support content-specific attritbutes.

Additionally, support for security attributes is defined in clause A.9, for use in secure environments.

Refer to the content-specific clauses for support for content-specific attributes.

6.5 Pragmatic constraints for attribute types

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

6.6 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 A.4.

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 5.

Table 5 - 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 14.10.

6.7 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.

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 6.

Table 6 - 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 14.10.

7 Remote user agent support

7.1 Introduction

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

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), and independent of any particular content type. The content-specific requirements for UAs are specified in the content-specific sections of this part of the Implementor’s Agreements.

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 Remote User Agent services and protocols. Access to a Message Store by a Remote User Agent is covered in clause 6.

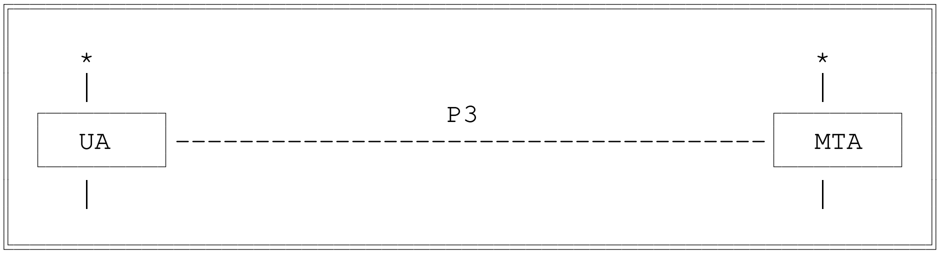

Figure 6 - Scope of remote user agent agreements

7.3 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 clause 5.2.

Support for Elements of Service is specified for the MT Service (table 7) and is in addition to the support requirements specified in clauses 5 and 13 if this Functional Group is supported.

Table 7 - 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

7.4 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.

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 8.

Table 8 - 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 14.10.

8 Naming, addressing & routing

8.1 Use of O/R addresses for routing

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

8.2 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, however, unrecognized DDA types may be ignored for these purposes.

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.

d) An extension attribute encoded as Teletex String shall be compared with the corresponding standard attribute encoded as Printable String if that extension attribute is not present in both ORAddresses. Matching rules are as specified in clause 18.4 of X.402 (1988) (as modified in the

MHS Implementors' Guide) except that only teletex graphic characters from repertoire no. 102 need to be compared for Printable String equivalence (i.e., the presence of graphic characters from other repertoires can be treated as a mismatch).

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.

8.3 Distribution lists

8.3.1 Introduction

This clause identifies and specifies the Distribution Lists Functional Group, which covers all issues relating to the performance of distribution list (DL) expansion by an MTA. Other aspects concerned with the **use** of distribution lists are covered in the MT Kernel Functional Group.

8.3.2 Elements of service

This clause specifies the requirements for support of Elements of Service for conformance to the Distribution Lists 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 for the MT Service only (table 9), and is only concerned with the performance of DL expansion by an MTA. Such support is in addition to the support requirements specified in clause 5 if this Functional Group is supported.

Table 9 - Distribution lists: MT elements of service

Element of Service	Support
DL Expansion History Indication	M
DL Expansion Prohibited	M
Use of Distribution List	M1
Notes 1 Use of DL Names is always possible because a DL name cannot be distinguished from any other OR Name on origination.	

8.4 MHS use of Directory

8.4.1 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.

8.4.2 Functional configuration

Two MHS functional entities, the 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.

8.4.3 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.

8.4.4 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 7.

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

Figure 7 - 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.

8.4.5 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 10).

Table 10 - Use of directory: MT elements of service

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

8.4.6 Directory services

These Implementation Agreements require the Directory services as defined in table 11. Indicated are the Directory services required to support the needs of the MHS UA/MTA and MHS Administrator.

Table 11 - 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	M
Modify RDN	O	O

8.4.7 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.

8.4.7.1 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.

8.4.7.2 Standard application specific attributes and attribute sets

The standard application specific attributes and attributes sets supported by these Implementation Agreements are listed in table 12. For each attribute and attribute set, a reference is provided to the standard where it is defined.

Table 12 - 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

8.4.7.3 Standard application specific object classes

The standard application specific object classes supported by these Implementation Agreements are listed in table 13. For each object class, a reference is provided to the standard where it is defined.

Table 13 - 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

8.4.7.4 OIW application specific attributes and attribute sets

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

8.4.7.5 OIW application specific object classes

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

8.4.7.6 Structure rules

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

8.4.7.6.1 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.

8.4.7.6.2 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.

8.4.7.7 Use of Capabilities Information

The capabilities information in the X.500 Directory should not be considered sufficient to warrant a non-delivery decision by an originating or relaying MTA. This clause is not intended to impose any conformance requirement.

8.5 Address support for Teletex character sets

This clause identifies the Address Support for Teletex Character Sets Functional Group, which covers the generation of Teletex strings in OR Address components.

Support of this functional group implies that, if an address component is supported for origination, the corresponding Teletex component (if any) must be supported for origination.

8.6 Reply support

When originating a reply, the UA must be able to utilize the applicable addressing components of the message to which it is replying (regardless of character set support level).

9 MHS management

NOTE - For further study.

10 MHS security

10.1 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 14 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 14 - 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 8.

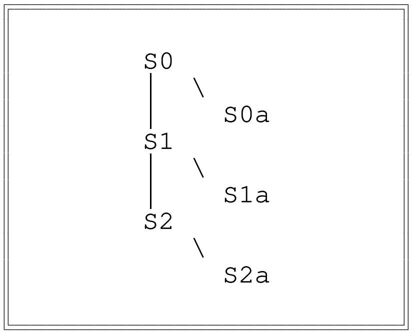

Figure 8 - Incremental functionality of the security classes

10.2 Common requirements

10.2.1 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 18) 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.

10.2.2 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.

10.2.3 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" (sec. 7.8.1 of X.228) on an existing, authenticated RTSE association owned by this MTA.

10.3 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 9 explains the column headings used in the security class tables. The classifications are defined in clause 5.2.

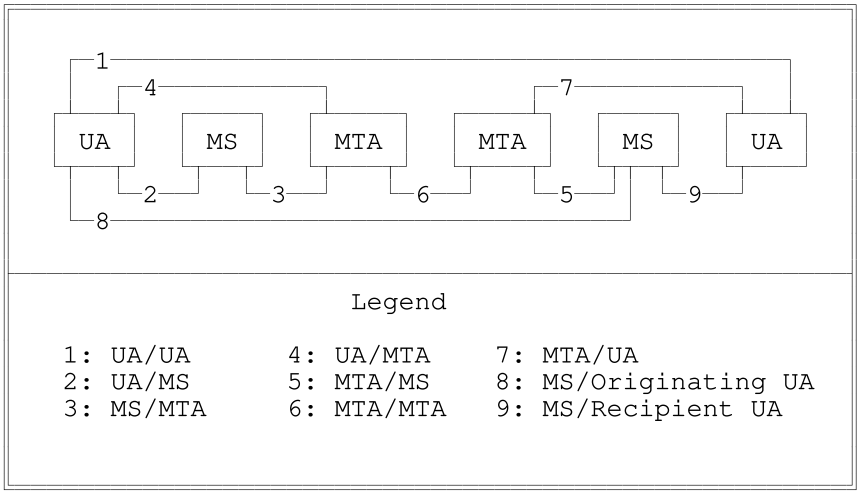

Figure 9 - Security interfaces

10.4 Security class 0 (S0)

10.4.1 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.

10.4.2 Security services for S0

Security class 0 (S0) mandates the security services listed in table 15.

Table 15 - Security class 0 (S0)

Security Interface	1	2	3	4	5	6	7	8	9
Security Service	UA/ UA	UA/ MS	MS/ MTA	UA/ MTA	MTA/ MS	MTA/ MTA	MTA/ UA	MS/ UA	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 15 - 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).

10.5 Security class 0A (S0a)

10.5.1 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; and,

b) Content Confidentiality.

10.5.2 Security services for S0a

Security class 0A (S0a) mandates the security services of class S0 plus those listed in table 16.

Table 16 - Security class 0A (S0a)

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

10.6 Security class 1 (S1)

10.6.1 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; and,

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.

10.6.2 Security services for S1

Security class 1 (S1) mandates the security servicesof class S0 plus those listed in table 17.

Table 17 - Security class 1 (S1)

Security Interface	1	2	3	4	5	6	7	8	9
Security Service	UA/ UA	UA/ MS	MS/ MTA	UA/ MTA	MTA/ MS	MTA/ MTA	MTA/ UA	MS/ UA	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.

10.7 Security class 1A (S1a)

10.7.1 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; and,

b) Content Confidentiality.

10.7.2 Security services for S1a

Security class 2A (S1a) mandates the security services of class S1 plus those listed in table 18.

Table 18 - 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	–	–	–	–	–	–	–	–

10.8 Security class 2 (S2)

10.8.1 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; and,

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

10.8.2 Security services for S2

Security class 2 (S2) mandates the security services of class S1 plus those listed in table 19.

Table 19 - 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).

10.9 Security class 2A (S2a)

10.9.1 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; and,

b) Content Confidentiality.

10.9.2 Security services for S2a

Security class 2A (S2a) mandates the services of class S2 plus those listed in table 20.

Table 20 - Security class 2A (S2a)

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

11 Specialized access

11.1 Physical delivery

This clause identifies and specifies the Physical Delivery Functional Group, which is intended to cover all issues relating to access to physical delivery systems by an MHS implementation.

11.1.1 Elements of service

This specifies the requirements for support of Elements of Service for conformance to the Physical Delivery 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 for:

a) the MT Service in table 21;

b) the O/R Address Attributes in table 22; and,

c) the character string support in table 23.

Editor's Note - table 23 does not appear in this part.

NOTE - All Elements of Service listed in table 21 are 1988.

Table 21 - Physical delivery: MT elements of service

Element of Service	UA Origination	PDAU Reception
Additional Physical Rendition	O	O
Basic Physical Rendition	M	M
Counter Collection	M	M
Counter Collection with Advice	O	O
Delivery via Bureaufax Service	O	O
EMS (Express Mail Service)	~~M~~O	~~M~~O
Ordinary Mail	M	M
Physical Delivery Notification by MHS	O	O
Physical Delivery Notification by PDS	O	O
Physical Forwarding Allowed	M	M
Physical Forwarding Prohibited	M	M
Registered Mail	O	O
Registered Mail to Addressee in Person	O	O
Request for Forwarding Address	O	O
Special Delivery	~~M~~O	~~M~~O
Undeliverable Mail with Return of Physical Message	M	M

Table 22 - Character string support

Character String	Origination (UA)	Reception (PDAU)
Printable	M	M
Teletex	O[1]	O[2]

Notes

1 Mandatory if "Address Support for Teletex Character Sets" functional group is supported.

2 Mandatory if "Address Support for Teletex Character Sets" functional group is supported, with a minimum of one character repertoire.

11.2 Other access units

11.2.1 Facsimile access units

NOTE - The possible development of Agreements in this area is for further study.

11.2.2 Telex access units

It is not currently intended to develop Agreements in this area.

11.2.3 Teletex access units

It is not currently intended to develop Agreements in this area.

12 Redirection

The redirection functional group is for further study.

13 IPM service

13.1 Introduction

This clause specifies the requirements for a minimal 1988-based IPMS implementation (i.e., IPM UA) which is capable of interworking with 1984-based UAs.

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 A.3, or MS Submission and Retrieval based on the protocol classifications in clause A.4. 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.

13.2 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 clause 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 23 and 24.

Table 23 - 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 24 - IPM kernel: IPM service optional user facilities

Element of Service[1]	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~~M	-
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	M
Non-receipt Notification Request	O	M[2]
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~~M	-
Redirection of Incoming Messages (1988)	-	O
Reply Request Indication	O	M
Replying IP-message Indication	M	M
Requested Delivery Method (1988)	~~M~~O	-

Table 25 - 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)	~~OM~~[3]	-

Notes

1 Other UA Elements of Service are listed in Table 4.

2 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.

3 Use of a DL on submission is always possible as DLs cannot be distinguished from other O/R addresses.

13.3 Interpersonal messaging protocol (P2)

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

13.4 Body part support

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

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 33 of Annex A of this part. 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. If an implementation supports origination of forwarded messages, it must be capable of forwarding every body part that is supported on reception. The reception requirements on the UA do not necessarily include the ability to render (display) all of the characters received. If the message is forwarded, the UA must transmit exactly equivalent characters, but not necessarily from the same character set.

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 10. 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.

```
BodyPart              ::=  CHOICE {
  ia5-text                 [0] IA5TextBodyPart,
                           .
  oda-1984                 [12] IMPLICIT OCTET STRING,
  iso-6937                 [13] ISO6937BodyPart,
  bilaterally-defined      [14] Unidentified,
  externally-defined       [15] ExternallyDefinedBodyPart,
                           .
                           .
                           [310] IMPLICIT
                                USAPrivatelyDefinedBodyParts,
                           .        }

Unidentified := OCTET STRING
```

The content of the ODA OCTET STRING will contain a value of type ODABodyPart as follows:

```
ODABodyPart ::= SEQUENCE {
   ODABodyPartParameters,
   ODAData }
```

The Parameters and Data components are defined in Annex E of CCITT Recommendation T.411 (1988) (ISO 8613-1).

USAPrivatelyDefinedBodyParts 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 10 - Privately-defined body parts

13.5 MS attributes

The IPM MS provides more flexible access to the general attributes (see clause A.8, table 43, enhanced column) as well as supporting IPM attributes (see clause A.10).

IPM UAs can make use of either the Basic MS or the IPM MS.

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

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

13.5.1 Implementation of the IPM 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.

13.6 Body part conversion functional group

13.6.1 General

The Body Part Conversion Functional Group supports the functionality required to perform the action of message body part conversion. The Element of Service "Conversion Prohibition" is made mandatory in the MT Kernel.

13.6.2 Elements of service

The Body Part Conversion Functional Group provides support for the following Elements of Service.

Table 25 - Conversion: MT elements of service

Element of Service	Support
Conversion Prohibition in Case of Loss of Information (1988)	M
Explicit Conversion	M[1]
Implicit Conversion	O[1]
Notes 1 At least one of explicit or implicit conversion must be supported for conformance to this functional group.	

Operational Notes
Conversions to and from General Text can only be performed through implicit conversion. Among possible implicit conversions are the following:

a) Teletex to General Text;

b) IA5 Text to General Text;

c) General Text to Teletex;

d) General Text to IA5 Text.

13.6.3 Conformance

An implementation conforming to this functional group shall conform to the procedures for the Elements of Service in clause 13.6.2, and shall obey the rules defined in clauses 14.3.5 and 14.3.9 of X.411 / ISO/IEC 10021-4.

The PICS shall document which body part conversions the implementation can perform, both for implicit and explicit conversion, and whether "Conversion Prohibition in Case of Loss of Information" is supported. Conformance to this functional group does not mandate conversion between any two specific body part types.

If conversion has to take place and the Element of Service "Conversion Prohibition in Case of Loss of Information" is requested, then the MTA is not allowed to perform the conversion if loss of information may occur, according to the classification in clause 2.1 of X.408.

If the General Text body part type is supported, the implementation must support two-way conversion between the General Text IA5 subrepertoire and the IA5 Text body part.

If a UA is registered to receive multiple Encoded Information Types and its MTA receives a message for it containing any of those registered EITs, the corresponding body parts shall not be converted prior to delivery.

13.7 Security

There are no security requirements to support IPM, above and beyond those specified in clause 10.

13.8 Error handling

NOTE - For further study.

13.9 Physical delivery

Table 26 specifies the support for physical delivery elements of service as required by IPM.

Table 26 - Physical delivery: IPM elements of service

Element of Service	Origination (IPM UA)	Reception (PDAU)
Additional Physical Rendition	O	O
Basic Physical Rendition	O[1]	M
Counter Collection	M	M
Counter Collection with Advice	O	O
Delivery via Bureaufax Service	O	O
EMS (Express Mail Service)	M	M[2]
Ordinary Mail	O[1]	M
Physical Delivery Notification by MHS	O	O
Physical Delivery Notification by PDS	O	M
Physical Forwarding Allowed	O[1]	M
Physical Forwarding Prohibited	M	M
Registered Mail	O	O
Registered Mail to Addressee in Person	O	O
Request for Forwarding Address	O	O
Special Delivery	M	M[2]
Undeliverable Mail with Return of Physical Message	O[1]	M

Notes

1 Provided by default (when using a physical delivery address).

2 Must support EMS and/or Special Delivery.

14 EDI messaging service

14.1 Introduction

This clause specifies the requirements for an EDI Messaging Service (EDIMS). These requirements are based on Recommendations X.435 and F.435 which define the P(edi) content type and outline various EDIMS operational scenarios.

This EDIMS Implementation Agreement separates the functions of the base standard into a Kernel and optional Functional Groups (FGs). These functional groups may be used to support the different scenarios of the EDIMS.

The following functional groups are defined:

- EDIMS Security

- EDIMS Forwarding

- EDIMS Multipart Body

- EDIMS Physical Delivery

These agreeements classify the support of these functional groups as follows:

Table 27 - EDIMS functional groups

Functional Group	Support
EDIMS Forwarding	O
EDIMS Security	O
EDIMS Multi Part Body	O
Notes	

14.2 EDIMS Elements of service

Tables 28.1 and 29 specify the requirements for support of EDIMS EoS by a UA conforming to the EDIMS functional group of this Agreement. The classification scheme for support of EoS is as defined in clause 5.2.

Table 28 - EDIMS: Basic EDI 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
EDI Message Identification	M	M
Message Identification	M	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 29 - EDIMS: Optional EDI elements of service

	Kernel		Func. Group		
Element of Service	Orig	Rec	FG	Orig	Rec
Alternate Recipient Allowed	M	M			
Alternate Recipient Assignment	-	O			
Application Security Element	O	O[1]	SEC-C	M	M
Character Set	M	M			
Content Confidentiality	O	O	SEC-A,B	C[7]	C
Content Integrity[5]	O	O	SEC-A,B	C[7]	C
Conversion Prohibition	M	M			
Conversion Prohibition in Case of Information Loss (1988)	O	O			
Cross Reference Information	O	M	MPB	M	M
Deferred Delivery	M	-			
Deferred Delivery Cancellation	M	-			
Delivery Notification	M	-			
Designation of Recipient by Directory Name	O	-			
Disclosure of Other Recipients	M	M			
DL Expansion History Ind.(1988)	-	M			
DL Expansion Prohibited	M	-			
EDI Forwarding	O	-	FWD	M	-
EDI Message Type(s)	M	M			
EDI Notification Request	M	M			
EDI Standard Indication	M	M			
EDIM Responsibility Forwarding Allowed Indication	M	M			
EDIN Receiver	O	M	FWD	M	M
Expiry Date/Time Indication	O	M			
Explicit Conversion	O	-			
Grade of Delivery Selection	M	M			
Hold for Delivery	-	O[4]			
Implicit Conversion	-	O			
Incomplete Copy Indication	O	M	FWD	O[2]	M
Interchange Header	M	M			
Latest Delivery Designation	O	-			
Message Flow Confidentiality	O	-			
Message Origin Authentication[5]	O	O	SEC-A,B	C[7]	C
Message Security Labelling	O	O	SEC-A,B	C[7]	C
Message Sequence Integrity	O	O			
Multi-Destination Delivery	M	-			
Multi-Part Body	O	M	MPB	M	M
Non-repudiation of Content Originated	O	O	SEC-B	M	M
Non-repudiation of Content Received	O	O	SEC-B	M	M
Non-repudiation of Content Received Request	O	O	SEC-B	M	M
Non-repudiation of Delivery	O	O	SEC-A,B	C[7]	C
Non-repudiation of EDI Notification	O	O	SEC-B	M	M
Non-repudiation of EDI Notification Request	O	O	SEC-B	M	M

Table 29 - EDIMS: Optional EDI elements of service (concluded)

	Kernel		Func. Group		
Element of Service	Orig	Rec	FG	Orig	Rec
Non-repudiation of Origin[6]	O	O	SEC-A,B	C[7]	C
Non-repudiation of Submission	O	O			
Obsoleting Indication	O	M			
Originator Indication	M	M			
Originator Requested Alternate Recipient (1988)	O	-			
Prevention of Non Delivery Notification	O	-			
Probe	O	-			
Probe Origin Authentication	O	-			
Proof of Content Received	O	O	SEC-A,B	M	M
Proof of Content Received Request	O	O	SEC-A,B	M	M
Proof of Delivery	O	O			
Proof of EDI Notification	O	O	SEC-A,B	M	M
Proof of EDI Notification Request	O	O	SEC-A,B	M	M
Proof of Submission	O	-			
Recipient Indication	M	M			
Redirection Disallowed by Originator	O	-			
Redirection of Incoming Messages (1988)	-	O			
Related Message(s)	O	M			
Report Origin Authentication	O	O			
Requested Delivery Method	M	-			
Restricted Delivery (1988)	-	O			
Return of Content[3]	O	-			
Secure Access Management	O	O			
Services Indication	O	O			
Stored EDI Message Auto-forward	-	O			
Use of Distribution List (1988)	O	-			

Notes

1 This EOS requires a bilateral agreement.

2 Mandatory when an implementation supports the removal of body parts.

3 A defect report was submitted to CCITT/ISO by EWOS/ETSI, since the Return of Contents EoS was omitted from the list of EDIMS EoS in F.435.

4 Mandatory if P3 is supported.

5 SEC-A or SEC-B EoS may require the use of these services.

6 SEC-B EoS may require the use of this service.

7 Support of this EOS is dependent on the MHS Security Class implemented to support security class EDI-A (SEC-A) or EDI-B (SEC-B). See clause 10.

14.3 P(EDI) protocol

The requirements for EDI-UA support of the EDI protocol (Pedi) elements are defined in clause A.11.

14.4 EDIMS Multi-Part Body functional group

14.4.1 General

The EDIMS Multi-Part Body functional group defines the services and functionality required to support the generation of multiple body parts in an EDIM. Note that support on reception of Multi-Part Body is mandatory in the EDIMS Kernel.

14.4.2 Elements of service

The EDIMS Multi-Part Body functional group constitutes support of the following Elements of Service on origination:

- Cross Reference Information

- Multi-Part Body

14.5 EDI Message Store (EDI-MS)

14.5.1 MS Attributes

14.6 Conversion

14.7 EDIMS security functional group

The EDIMS Security functional group defines the services and functionality required to provide security for EDIMs and EDINs. These security features are specific to the EDIMS, and are described in X.435.

As the interface between the EDI Messaging (EDIMG) user and the EDI-UA is outside the scope of this document, implementations of the security mechanisms can be implemented as a discrete hardware/software component or within the EDI-UA.

> **NOTE -** There are alternative methods of providing security to the EDIMG user. For example, the EDI-UA may just avail itself of the (content-type independent) security services provided or supported by the (1988) MHS and described in section 10 (e.g., content confidentiality, proof of delivery), without using the additional services of this functional group. Finally, security services may be provided within the EDI interchange itself, while possibly using the EDI Application Security Element to convey some (bilaterally agreed) security

arguments (e.g., key IDs) in the EDIM header.

The EDIMS Security functional group is specified as two security classes, denoted EDI-A and EDI-B. Note that the services provided below are provided, in some cases, by 1988 MHS security elements in the P1 (and P3) envelope. For example, depending on the security policy in force, the proof and non repudiation services below use the Content Integrity Check or Message Origin Authentication Check protocol elements.

See Section 10 of these Agreements for a description of the 1988 MHS Security functional group and classes. Annex A of these Agreements outlines support of the security protocol elements by the MTS.

The security classes EDI-A and EDI-B need the Message Origin Authentication and Content Integrity EoS. This shall be achieved either by supporting security class S0, or any other security class in clause 10, depending on the security policy in force.

> **NOTE -** In order to counter the threat that a message could be stolen and its value credited to a third party, the use of content confidentiality is recommended. When using S0A, the base security EoS shall be used in the following way:
>
> - the Content integrity check shall be generated from the clear content;
> - the Content integrity check shall be carried in the message token;
> - Content confidentiality shall be used. Encryption of the content prevents re-generation of the Content integrity check by a third party.

14.7.1 EDIMS security class EDI-A (SEC-A)

This class provides proof services; the recipient of an EDI information object can be assured that it was originated by the specified EDIMG user. Table 29 outlines support for the EoS contained in this class.

14.7.2 EDIMS security class EDI-B (SEC-B)

This class provides non repudiation services. These are "stronger" than the corresponding proof services in the sense that the recipient of an EDI information object can prove to a third party that the object was originated by the specified EDIMG user. Table 29 outlines support for the EoS contained in this class.

14.7.3 EDIMS security class EDI-C (SEC-C)

The security class EDI-C offers the following Element of Service:

- Application Security Element

This security class mandates that the above service is provided by an EDIMS end system.

14.8 EDIMS Physical Delivery functional group

14.9 EDIMS Forwarding functional group

14.9.1 General

The EDIMS Forwarding functional group defines the services and functionality required to perform forwarding of an EDI message by or on behalf of an EDIMG user.

An EDI-UA or EDI-MS claiming conformance to the EDI Forwarding functional group shall understand the semantics of the EDIMS abstract operations and service with regard to forwarding, EDI Notifications and EDIN reasons/diagnostic codes. The EDI-UA or EDI-MS shall generate appropriate EDI notifications when accepting, forwarding, or refusing responsibility for the EDI message. These notifications may be generated automatically by an EDI-MS or EDI-UA based on the presence or absence of an EDI-MS in the configuration. In addition, notifications may be generated as a result of a request by the EDIMG user. Please refer to Section 17.3.3 of X.435 for a full description of EDI Forwarding.

An EDI-UA that claims conformance to the EDIMS Forwarding functional group shall conform to clause A.12, Table 47, as regards protocol elements required by this functional group.

14.9.2 Elements of service

The EDIMS Forwarding functional group constitutes support of the following Elements of Service:

- EDI Forwarding

- EDIN Receiver

Conditional on the support of removal of body parts, the EDIMS Forwarding functional group offers the additional element of service:

- Incomplete Copy Indication

14.10 Use of Directory

15 Use of underlying layers

15.1 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.

15.2 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.

16 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.

16.1 PDU encoding

Various distinguished integer values will be defined in future versions of the X.400 standard that are not defined in the 1988 version. When an unknown distinguished value is encountered in an integer or an enumerated type, it should, in general, not result in an error. The value should be treated transparently or ignored, wherever possible.

> **Editor's Note -** It is intended that this section will specify any special error handling required when unknown distinguished values are encountered.

16.2 Envelope

NOTE - For further study.

16.3 Reports

NOTE - For further study.

16.4 Pragmatic constraints

If an implementation detects a pragmatic constraint violation, then it may generate an appropriate error indication but is not required to do so.

17 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 1) are listed in table 30. An implementation may claim conformance to multiple configuration types (e.g. "MTA+UA" and "Class B MTA only").

Table 30 - 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	–	–	–	–
Message Store[4]	–	M	–	–	–	M	M	M	–
Remote UA	–	–	–	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
Redirection	*	*	*	*	*	*	*	*	*
Physical Delivery	*	*	*	*	*	*	*	*	*
Other Access Units	*	*	*	*	*	*	*	*	*
IPM Service[6]	O[5]	O	O	O	O	O[5]	O	O[5]	O[5]
EDI Service[6]	O[5]	O	O	O	O	O[5]	O	O[5]	O[5]

Notes

1 There are three conformance classes defined for the MT Kernel in clause 17.1.

2 Optional elements of a context-specific UA 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 17.2 for MS support.

5 At least one of the content-specific functional groups must be supported.

6 The content-specific functional groups may include requirements for levels of support by an MS and/or MTA (e.g., in terms of attributes supported, conversion requirements, etc.). In table 29, the support of a content-specific functional group by the MS only implies support of the MS requirements for that content type (i.e., attribute). Similarly, support in the MTA for a content-specific functional group only implies support for the MTA requirements for that content type (e.g., conversion).

17.1 MT Kernel Conformance Classes

The MT Kernel conformance classes 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.

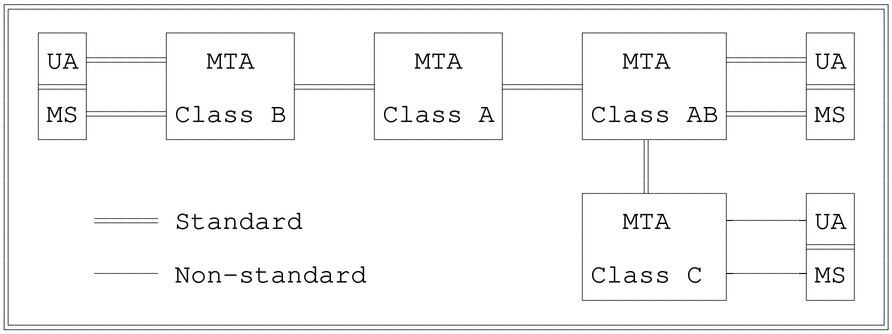

Figure 11 - MT kernel conformance classes

17.2 MS conformance levels

The MS conformance levels are:

a) A Basic MS only requires support for the General Attributes as specified in clause A.8, basic column of table 43;

b) An enhanced MS requires support for more of the General Attributes as specified in clause A.8 (enhanced column);

c) A Secure MS additionally requires support for the attributes as specified in clause A.9.

For content-specific MS requirements, see the appropriate content-specific clauses.

17.3 EDI-UA conformance

The EDI functional group requires the support of the EDIFACT and ANSI X12 EDI syntaxes.

18 Management domain agreements

The sections above describe agreements among implementors of particular X.400 components (e.g., MTAs, UAs, MSs). There are some agreements that don't apply to a single X.400 component, but instead apply to an entire domain of X.400 components. This section details any requirements for X.400 domains, independent of those for individual X.400 components. A single X.400 component cannot be conformance tested for these domain requirements, but for a domain to claim to be "operationally OIW compliant," it must abide by the rules stated below.

18.1 Management domain names

This section contains requirements on matters being considered by the U. S. CCITT Study Group D for national decisions. Such decisions are likely to supersede the relevant portions of this clause.

The Implementation Agreements for 1984-based MHS implementations requires that all Management Domain Names (both Private and Administration) shall be unique within the U. S. This is also a requirement for 1988-based MHS implementations.

A "Construction Syntax" is defined, which uses a registered OSI Organization Name from the ANSI US Register of Organization Names as a "root" in the construction of MHS Management Domain Names e.g., ADMD and PRMD). The constructed combinations based on this "root" will be guaranteed to be unique, and thus be safely used as MHS MD names in the United States. Other countries may wish to adopt these same rules.

MHS MD (PRMD and ADMD) names shall be constructed according to the Extended BNF grammar shown in figure 12.

```
<ADMDName> ::= <MDName>

<PRMDName> ::= <MDName>

<MDName> ::=
    <NationalOrganizationName> |
    <ConstructedName> |
    <NationalOrganizationNumber>

<ConstructedName> ::=
    <NationalOrganizationName>"+"<OrganizationallyDeterminedPart>
```

Figure 12 - Management domain name construction

Subject to all of the following rules:

Rule 1. The entire <MDName> must not exceed 16 bytes (including any constructor operators that may be included, and shall be composed entirely of PrintableString characters.

Rule 2. The <NationalOrganizationName> shall be drawn from the alphanumeric names registered in the US Register. It shall contain at least one non-numeric character, and not contain the constructor operator "+" (plus sign).

Rule 3. Each <NationalOrganizationName> obtained from the US Registry will be accompanied by a NumberForm (numeric value) which shall be bound as the <NationalOrganizationNumber> to the <NationalOrganizationName>.

Rule 4. In a <ConstructedName>, the <OrganizationallyDeterminedPart> shall be certified to be unique under the <NationalOrganizationName> (sub)authority, by the <NationalOrganizationName> registration authority.

Rule 5. A <NationalOrganizationNumber> shall be obtained from the US Register and bound to the <ConstructedName>.

Rule 6. A Private Management Domain's PrivateDomainIdentifier shall be the same as its PrivateDomainName.

NOTES

1 The PRMD names resulting from the <ConstructedName> syntax (those having a "+" in them) are atomic values from the point of view of the MTA -- in particular, it is not permissible for the MTA to route on components of the PRMD name.

2 The construction rules are such that if ABC is a Registered National Organization Name, then the owner of that name controls the MHS Domain Name space including "ABC" and "ABC+<anything>," but not "ABC<anything>."

3 A "+" is legal in an ANSI provided name.

4 If a Registered Organization Name already contains the construction operator ("+" sign), then in order to use the name as an <MDName>, its owner must also register the "root" which precedes the first "+" sign, with the US Register of Organization Names. (e.g., company B+Z+P would need to register "B" to be able to use the "constructed" name of B+Z+P.)

5 For the special case of the construction operator ("+" sign) being the first character of a Nationally Registered Name, no special action is required beyond its normal registration with the US Registry of Organization Names.

6 If the sub-authority determined by <NationalOrganizationName> so wishes, the <OrganizationallyDeterminedPart> can be constructed using rules similar to the above, resulting in a hierarchical construction separated by "+"s. In particular, the sub-authority must maintain its own registry and might (for example) define the <OrganizationallyDeterminedPart> using the syntax

```
<OrganizationallyDeterminedPart>  ::=  <DivisionName>
       │  <DivisionName> "+" <DivisionallyDeterminedPart>
```

Figure 13 - Name construction by subauthorities

where the <DivisionName> is drawn from the sub-authority's registry (and does not contain a "+"). Thus the sub-authority can delegate the use of the prefix

```
<NationalOrganizationName>+<DivisionName>
```

Figure 14 - Prefix

to someone else.

18.2 Use of ADMD names

This subsection was developed by an X.400 SIG working group in April, 1990. It contains extremely controversial positions that invoke national, commercial, and quality of service issues. The OIW may not be the correct forum to make these national decisions. Until these decisions can be reached or a national forum established, this section remains as a placeholder in the OIW X.400 SIG Working Text document only.

> **NOTE -** Version 2 of the CCITT X.400 Implementors Guide, dated 16 March 1990, allows for a single zero ("0") character as the ADMD name for the case of a PRMD that is not reachable from any ADMD. The following discussion does not apply to such PRMDs.

A PRMD may be directly connected to more than one ADMD. Since a PRMD may not alter the originators ORAddress, the Country/ADMD name pair provided in the Originator ORAddress may not match those of the first ADMD to receive the message from the PRMD. The first ADMD is required to accept such messages and may not alter the originator's ORAddress.

Any message originated by a PRMD must have an Originator's ORAddress that either uses the single space ADMD name or uses a Country/ADMD name pair for an ADMD to which the PRMD is connected. (In both cases the Country name is required.)

The X.400 Recommendations have defined a mechanism that enables PRMDs connected to multiple ADMDs to enter a single space as the ADMD name. To support this, these agreements recognize two classes of ADMDs. ADMDs in the first class, "space-supporting" ADMDs, must be able to route on PRMD name, independently from the ADMD name. Furthermore, the space-supporting ADMDs must arrange their routing configuration such that all PRMDs are reachable from all ADMDs. PRMDs using the single space ADMD name must be connected to at least one space-supporting ADMD.

ADMDs in the other class, "non-space-supporting" ADMDs, must, at a minimum, route messages for which the ADMD name is a single space to a space-supporting ADMD (in the indicated country). It is hoped that in the long term, all ADMDs will be able to route on the PRMD name when the ADMD name is a single space.

18.3 Uniqueness of MTS Identifiers within a management domain

When generating an IA5String in an MTS Identifier, each MTA in a domain must ensure that the string is unique within the domain. This shall be done by providing an MTA designator with a length of 12 octets which is unique within the domain, to be concatenated to a per message string with maximum length of 20 octets.

Two pieces of information, the MTA name and MTA designator, need to be registered within an MD to guarantee uniqueness. This registration facility need not be automated. If the MTA name is less than or equal to 12 characters, it is recommended that it also be used as the MTA designator.

Annex A (normative)

MHS protocol specifications

Tables 31 through 48 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 (32-48), 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 former classifications relate to the classifications in Part 7 of the Stable Agreements as shown in table 31.

Table 31 - 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 (32-48). 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.

There are two types of tables defining support for protocol elements: the first is a base table that contains and classifies all protocol elements, and the second is a delta table for a functional group.

Functional group tables need only list those protocol elements for which the functional group has changed the support requirements from the base table. Additional containing constructor elements may be listed in order to provide context information.

If the functional group changes the support requirements for a given element it must be classified in the delta table. Changes should only place more restrictions on the required support, for example changing an optional element to be either mandatory, excluded, or out of scope. If an element in the delta table is not classified, it is only listed for context information and the required support for it is the same as its classification in the base table.

The Dynamic column is only filled in if the profile changes the requirements for use of the element in every PDU, for example, if support for the element is required, but use of the element is optional in a given PDU. However, if you are supporting a functional group that element will always (or never) be used.

A.1 MTS transfer protocol (P1)

Within Table 32, the columns under "Support by MT Kernel Class" refer to the MT Kernel Conformance Classes defined in clause 17.1.

Table 32 - Classification of the P1 protocol elements

MTS Transfer Protocol (P1)				Part 1 of 9
Support by MT Kernel Class				Comments/References
		B/C	A	
Protocol Element	S	O/R	O/R	See Note 1
Operations				
MTABind	M	M/M	M/M	MTABind
MTAUnbind	M	M/M	M/M	
MTSE				
MessageTransfer	M	M/M	M/M	
ProbeTransfer	M	M/M	M/M	
ReportTransfer	M	M/M	M/M	See Note 7
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	
MTS-APDU				
message	M	M/M	O/M	
envelope	M	M/M	M/M	MessageTransferEnvelope
content	M	M/M	M/M	
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	

Table 32 - Classification of the P1 protocol elements (continued)

MTS Transfer Protocol (P1)				Part 2 of 9
Support by MT Kernel Class				Comments/References
Protocol Element	S	B/C O/R	A O/R	See Note 1
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	
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	

Table 32 - Classification of the P1 protocol elements (continued)

MTS Transfer Protocol (P1)				Part 3 of 9
	Support by MT Kernel Class			Comments/References
		B/C	A	
Protocol Element	S	O/R	O/R	See Note 1
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	
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

Table 32 - Classification of the P1 protocol elements (continued)

MTS Transfer Protocol (P1)				Part 4 of 9
	Support by MT Kernel Class			Comments/References
Protocol Element	S	B/C O/R	A O/R	See Note 1
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	
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	OriginatorAndDLExpansionHistory
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

Table 32 - Classification of the P1 protocol elements (continued)

MTS Transfer Protocol (P1)				Part 5 of 9
Support by MT Kernel Class				Comments/References
		B/C	A	
Protocol Element	S	O/R	O/R	See Note 1
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	
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	
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	

Table 32 - Classification of the P1 protocol elements (continued)

MTS Transfer Protocol (P1)				Part 6 of 9
Support by MT Kernel Class				Comments/References
		B/C	A	
Protocol Element	S	O/R	O/R	See Note 1
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	
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	

Table 32 - Classification of the P1 protocol elements (continued)

MTS Transfer Protocol (P1)				Part 7 of 9
Support by MT Kernel Class				Comments/References
		B/C	A	
Protocol Element	S	O/R	O/R	See Note 1
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	
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	
OriginatorAndDLExpansionHistory				
originator-or-dl-name	M	M/M	M/M	
origination-or-expansion-time	M	M/M	M/M	
RedirectionHistory				
Redirection	M	M/M	M/M	
intended-recipient-name	M	M/M	M/M	
ORAddressAndOptionalDirectoryName	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	O/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	

Table 32 - Classification of the P1 protocol elements (continued)

MTS Transfer Protocol (P1)				Part 8 of 9
Support by MT Kernel Class				Comments/References
Protocol Element	S	B/C O/R	A O/R	See Note 1
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	
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

Table 32 - Classification of the P1 protocol elements (concluded)

MTS Transfer Protocol (P1)				Part 9 of 9
	Support by MT Kernel Class			Comments/References
		B/C	A	
Protocol Element	S	O/R	O/R	See Note 1
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

1 The MT Kernel implementation classes are defined in clause 17.1.

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.

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.

6 In secure messaging, use of elements within the message token is preferred to use of equivalent elements in the subject message envelope. A security policy shall define which other elements are dynamically mandated and shall define which message security labels are used for security context checking.

7 In the absence of any specific processing requirements for a particular element in the Message Transfer or Probe Transfer, the action to be taken is simply the creation of the corresponding element in the Report Transfer and is subject to constraints specified in X.411.

A.2 Interpersonal messaging protocol (P2)

Table 33 - 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	ORDescriptor
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 33 - 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/M	
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 33 - Classification of the P2 protocol elements (concluded)

Interpersonal Messaging Protocol (P2)			Part 3 of 3
	Support by UA		
Protocol Element	S	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	See Note 10
parameters	M	M/M	
data	M	M/M	
GeneralTextBodyPart	O	O/M	See Note 9
ODA1984BodyPart	O	O/O	
ISO6937BodyPart	O	O/O	
BilaterallyDefinedBodyPart	O	O/O	
USAPrivatelyDefinedBodyPart	O	O/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.

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.

9 If General Text is supported, an implementation's PICS must identify which character repertoires can be generated on origination and supported on reception.

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

Editor's Note - The draft text note regarding the meaning of "support" on reception was missing from the editing instructions.

A.3 MTS access protocol (P3)

NOTE - The support classifications for the 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 34 - Classification of the P3 protocol elements

MTS Access Protocol (P3)					Part 1 of 12
Support by:					
		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
					See Note 10
delivery-control	M	M/-	M/-	-/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 34 - Classification of the P3 protocol elements (continued)

MTS Access Protocol (P3)					Part 2 of 12
	Support by:				
		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	-/M	-/M	M/-	
initiator-credentials	M	-/M	-/M	M/-	
simple	O	-/M	-/M	M/-	
strong	O	-/O	-/O	O/-	
security-context	O	-/O	-/O	O/-	
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	
RESULT					
responder-name	M	-/M	-/M	M/-	
mTS-user	-	-/-	-/-	-/-	
mTA	O	-/M	-/M	M/-	
isMessageStore	-	-/-	-/-	-/-	
messages-waiting	O	-/M	-/M	M/-	
responder-credentials	M	-/M	-/M	M/-	
simple	O	-/M	-/M	M/-	
strong	O	-/O	-/O	O/-	

Table 34 - Classification of the P3 protocol elements (continued)

MTS Access Protocol (P3)					Part 3 of 12
	Support by:				
		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/-	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/-	MTSIdentifier
probe-submission-time	M	-/M	-/M	M/-	
content-identifier	O	-/M	-/M	M/-	
CancelDeferredDelivery					
ARGUMENT					
message-submission-identifier	M	M/-	M/-	-/M	MTSIdentifier
SubmissionControl					
ARGUMENT					
controls	M	-/M	-/M	M/-	See Note 1
restrict	O	-/M	-/M	M/-	
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	
waiting-messages	O	O/-	O/-	-/M	
waiting-content-types	O	O/-	O/-	-/M	
waiting-encoded-information-types	O	O/-	O/-	-/M	EncodedInformationTypes

Table 34 - Classification of the P3 protocol elements (continued)

MTS Access Protocol (P3)					Part 4 of 12
	Support by:				
Protocol Element	S	UA O/R	MS O/R	MTA 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	M/-	M/-	-/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	EncodedInformationTypes
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/-	EncodedInformationTypes
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	EncodedInformationTypes
deliverable-maximum-content-length	O	O/-	M/-	-/M	
default-delivery-controls	O	O/-	O/-	-/O	
restrict	O	O/-	O/-	-/M	

Table 34 - Classification of the P3 protocol elements (continued)

MTS Access Protocol (P3)					Part 5 of 12
	Support by:				
		UA	MS	MTA	
Protocol Element	S	O/R	O/R	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	
permissible-encoded-information-types	O	O/-	O/-	-/M	EncodedInformationTypes
deliverable-content-types	O	O/-	M/-	-/M	
labels-and-redirections	O	O/-	O/-	-/O	
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	ORName
original-encoded-information-types	O	M/-	M/-	-/M	EncodedInformationTypes
content-type	M	M/-	M/-	-/M	
built-in	O	O/-	M/-	-/M	
external	O	O/-	M/-	-/M	
content-identifier	O	O/-	M/-	-/M	
priority	O	M/-	M/-	-/M	All values
per-message-indicators	O	M/-	M/-	-/M	
disclosure-of-recipients	O	O/-	M/-	-/M	

Table 34 - Classification of the P3 protocol elements (continued)

MTS Access Protocol (P3)					Part 6 of 12
	Support by:				
		UA	MS	MTA	
Protocol Element	S	O/R	O/R	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	O/-	O/-	-/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/-	O/-	-/M	MS Abstract Service only
PerRecipientMessageSubmissionFields	M	M/-	M/-	-/M	
recipient-name	M	M/-	M/-	-/M	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	O/-	O/-	-/O	Note 9
physical-forwarding-prohibited	O	O/-	O/-	-/O	
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 34 - Classification of the P3 protocol elements (continued)

MTS Access Protocol (P3)					Part 7 of 12
	Support by:				
		UA	MS	MTA	
Protocol Element	S	O/R	O/R	O/R	Comments/References
ProbeSubmissionEnvelope					See Note 6
originator-name	M	M/-	M/-	-/M	ORName
original-encoded-information-types	O	M/-	M/-	-/M	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	
content-length	O	M/-	M/-	-/M	
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	M/-	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	
PerRecipientProbeSubmission Fields	M	M/-	M/-	-/M	
recipient-name	M	M/-	M/-	-/M	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/-	O/-	-/O	See Note 9
physical-rendition-attributes	O	O/-	O/-	-/O	
MessageDeliveryEnvelope					See Note 7
message-delivery-identifier	M	-/M	-/M	M/-	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/-	
external	O	-/M	-/M	M/-	
originator-name	M	-/M	-/M	M/-	ORName

Table 34 - Classification of the P3 protocol elements (continued)

MTS Access Protocol (P3)					Part 8 of 12
	Support by:				
Protocol Element	S	UA O/R	MS O/R	MTA O/R	Comments/References
original-encoded-information-types	O	-/M	-/M	M/-	EncodedInformationTypes
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/-	ORName
this-recipient-name	M	-/M	-/M	M/-	ORName
originally-intended-recipient-name	O	-/M	-/M	M/-	ORName
converted-encoded-information-types	O	-/M	-/M	M/-	EncodedInformationTypes
message-submission-time	M	-/M	-/M	M/-	
content-identifier	O	-/M	-/M	M/-	
extensions	O	-/M	-/M	M/-	
conversion-with-loss-prohibited	O	-/M	-/M	M/-	
requested-delivery-method	O	-/M	-/M	M/-	See 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/-	
dl-expansion-history	O	-/M	-/M	M/-	

Table 34 - Classification of the P3 protocol elements (continued)

MTS Access Protocol (P3)					Part 9 of 12
	Support by:				
Protocol Element	S	UA O/R	MS O/R	MTA O/R	Comments/References
ReportDeliveryEnvelope					See Note 7
subject-submission-identifier	M	-/M	-/M	M/-	MTSIdentifier
content-identifier	O	-/O	-/O	M/-	
content-type	O	-/M	-/M	M/-	
built-in	O	-/M	-/M	M/-	
external	O	-/M	-/M	M/-	
original-encoded-information-types	O	-/M	-/M	M/-	EncodedInformationTypes
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/-	OriginatorAndDLExpansionHistory
reporting-DL-name	O	-/M	-/M	M/-	
reporting-MTA-certificate	O	-/O	-/O	O/-	
report-origin-authentication-check	O	-/O	-/O	O/-	
PerRecipientReportDeliveryFields	M	-/M	-/M	M/-	
actual-recipient-name	M	-/M	-/M	M/-	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/-	EncodedInformationTypes
originally-intended-recipient-name	O	-/M	-/M	M/-	ORName
supplementary-information	O	-/M	-/M	M/-	
extensions	O	-/M	-/M	M/-	
redirection-history	O	-/M	-/M	M/-	RedirectionHistory
physical-forwarding-address	O	-/O	-/O	O/-	
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/-	-/M	CountryName
administration-domain-name	O	M/-	M/-	-/M	DomainName
network-address	O	M/-	M/-	-/M	
terminal-identifier	O	M/-	M/-	-/M	

Table 34 - Classification of the P3 protocol elements (continued)

MTS Access Protocol (P3)					Part 10 of 12
Support by:					
		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	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	O/-	O/-	-/M	
teletex-organization-name	O	O/-	O/-	-/M	
teletex-personal-name	O	O/-	O/-	-/M	
teletex-organizational-unit-names	O	O/-	O/-	-/M	
teletex-domain-defined-attributes	O	O/-	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 34 - Classification of the P3 protocol elements (continued)

MTS Access Protocol (P3)					Part 11 of 12
	Support by:				
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 34 - Classification of the P3 protocol elements (concluded)

MTS Access Protocol (P3)					Part 12 of 12
	Support by:				
Protocol Element	S	UA O/R	MS O/R	MTA O/R	Comments/References
EncodedInformationTypes					
built-in-encoded-information-types	M	M/M	M/M	M/M	See Note 3
non-basic-parameters	O	O/O	O/O	O/O	
external-encoded-information-types	O	O/M	O/M	M/O	
MTSIdentifier					
global-domain-identifier	M	M/M	M/M	M/M	GlobalDomainIdentifier
local-identifier	M	M/M	M/M	M/M	
OriginatorAndDLExpansionHistory					
originator-or-dl-name	M	M/M	M/M	M/M	
origination-or-expansion-time	M	M/M	M/M	M/M	
RedirectionHistory					
Redirection	M	M/M	M/M	M/M	
intended-recipient-name	M	M/M	M/M	M/M	
ORAddressAndOptionalDirectoryName	M	M/M	M/M	M/M	ORName
redirection-time	M	M/M	M/M	M/M	
redirection-reason	M	M/M	M/M	M/M	

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.

10 In the absence of any specific processing requirements for a particular element in the Message Submission, or Probe Submission, the action to be taken is simply the creation of the corresponding element in the ReportDelivery (subject to any constraints specified in X.411).

11 Applicable only to reception by a PDAU.

A.4 MS access protocol (P7)

Table 35 - Classification of the P7 protocol elements

MS Access Protocol (P7)				Part 1 of 6
Support by:				
		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	Opt'l in Basic MS(Note 5)
allowed-content-types	O	O/-	-/M	
allowed-EITs	O	O/-	-/M	
maximum-content-length	O	O/-	-/M	
MS-configuration-request	O	O/-	-/M	

Table 35 - Classification of the P7 protocol elements (continued)

MS Access Protocol (P7)				Part 2 of 6
Support by:		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	-/O	M/-	
available-attribute-types	O	-/O	M/-	
alert-indication	O	-/O	O/-	
content-types-supported	O	-/O	M/-	
Summarize				
ARGUMENT				
SummarizeArgument	M	M/-	-/M	
information-base-type	O	O/-	-/M	InformationBase
selector	M	M/-	-/M	Selector
summary-requests	O	O/-	-/M	
RESULT				
SummarizeResult	M	-/M	M/-	
next	O	-/M	M/-	
count	M	-/M	M/-	
span	O	-/M	M/-	
lowest	M	-/M	M/-	
highest	M	-/M	M/-	
summaries	O	-/M	M/-	
absent	O	-/M	M/-	
present	O	-/M	M/-	
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	O/-	-/M	AttributeSelection
RESULT				
ListResult	M	-/M	M/-	
next	O	-/M	M/-	
requested	O	-/M	M/-	EntryInformation

Table 35 - Classification of the P7 protocol elements (continued)

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

Table 35 - Classification of the P7 protocol elements (continued)

MS Access Protocol (P7)				Part 4 of 6
Support by:				
		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	-/O	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	M/-	-/M	See P3 MessageSubmission -Envelope
deferred-delivery-time	O	O/-	-/M	
extensions	O	O/-	-/M	See P3 MessageSubmission -Envelope
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 MessageSubmission -Envelope
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	M/-	-/M	AttributeSelection

Table 35 - Classification of the P7 protocol elements (continued)

MS Access Protocol (P7)				Part 5 of 6
	Support by:			
		UA	MS	
Protocol Element	S	O/R	O/R	Comments/References
Common Data Types				
AttributeSelection				
type	M	M/-	-/M	
from	O	O/-	-/M	
count	O	O/-	-/M	
AttributeValueAssertion				
type	M	M/-	-/M	
value	M	M/-	-/M	
EntryInformation				
sequence-number	M	-/M	M/-	
attributes	O	-/M	M/-	
type	M	-/M	M/-	
values	M	-/M	M/-	
Filter				
item	O	M/-	-/M	FilterItem
and	O	O/-	-/M	See Note 3
or	O	O/-	-/M	See Note 3
not	O	M/-	-/M	See Note 4
FilterItem				
equality	O	O/-	-/M	AttributeValueAssertion (Support is Optional 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 35 - Classification of the P7 protocol elements (concluded)

MS Access Protocol (P7)				Part 6 of 6
	Support by:			
Protocol Element	S	UA O/R	MS O/R	Comments/References
Range				See Note 6
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	M/-	-/M	
override	O	M/-	-/M	Opt'l in Basic MS-Note 5

Notes

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

2 The specified syntax of other-parameters is context-specific - see X.413 section 12.1.

3 For recursive use of filter, only support of the "item" and the "not" fields is required; there is only one level of recursion.

4 For recursive use of filter, only support of the "item" field is required; there is only one level of recursion.

5 If one of fetch-restrictions of MSBind and override of Selector is implemented, the other must also be implemented.

6 At least one of From or To must be implemented.

A.5 Classification of the P1 protocol elements for security classes

The protocol element classifications used in tables 36 and 37 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 33. Thus, table 36 shows the additional support required in P1 to conform to security class S1. Table 37 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 36 - 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				
	B/C	A		
Protocol Element	O/R	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 36 - 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				
	B/C	A		
Protocol Element	O/R	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 37 - 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				
	B/C	A		
Protocol Element	O/R	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 37 - 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				
	B/C	A		
Protocol Element	O/R	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 38, 39, and 40 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 P3 to conform to security class S0. Table 39 indicates the additional support required to support security class S1 (above and beyond that for security class S0). Table 40 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 38).

Table 38 - 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:					
Protocol Element	UA O/R	MS O/R	MTA O/R	Dyn	Comments/References
MessageDelivery					
RESULT					
proof-of-delivery	M/-	M/-	-/O		
MessageSubmissionEnvelope					
PerRecipientMessageSubmissionFields					
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 38 - 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:					
	UA	MS	MTA		
Protocol Element	O/R	O/R	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 39 - 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:					
	UA	MS	MTA		
Protocol Element	O/R	O/R	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 39 - 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:	UA	MS	MTA		
Protocol Element	O/R	O/R	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 39 - 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:					
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 40 - 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:					
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 40 - 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:	UA	MS	MTA		
Protocol Element	O/R	O/R	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 41 presents the classification delta to classification tables 38, 39, and 40, 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 41 - 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:	UA	MS	MTA		
Protocol Element	O/R	O/R	O/R	Dyn	Comments/References
MessageSubmissionEnvelope					
extensions					
content-confidentiality-algorithm-identifier	M/-	O/-	-/O		See Note 1
message-token					
asymmetric-token					
signed-data	M/-	-/-	-/-		
content-confidentiality-algorithm-identifier	M/-	-/-	-/-		See Note 1
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	-/-		See Note 1
encrypted-data					
content-confidentiality-key	-/M	-/M	-/-		
content-confidentiality-algorithm-identifier	-/M	-/M	O/-		See Note 1

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 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 35. Thus, table 42 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 42 - 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:	UA	MS		
Protocol Element	O/R	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 43 specifies the classification of the Message Store General Attributes.

Table 43 - Classification of the message store general attributes

Message Store General Attribute Support					Part 1 of 2
Support by:			Bas	Enchanced	
		UA	MS	MS	
Attribute	S	R	O	O	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	M	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	M	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	M	M	
parent-sequence-number	M	M	M	M	
per-recipient-report-delivery-fields	M	M	M	M	
priority	O	O	M	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	M	
reporting-mta-certificate	O	O	O	O	

Table 43 - Classification of the message store general attributes (concluded)

Message Store General Attribute Support					Part 2 of 2
Support by:	UA		Bas MS	Enhanced MS	
Attribute	S	R	O	O	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 MS General Attributes for Security Classes

The classification of the attributes in table 44 is a delta to the Enhanced MS column of the MS General Attributes in table 43. Table 44 indicates the additional attributes that must be supported in the MS for each of the security classes. There is no support required for security attributes in the basic MS.

Table 44 - 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

Table 45 specifies the classification of the Message Store IPM attributes. This clause is to be read in accordance with Annex C of X.420 (1988). For support of MS General Attributes, see table 43, enhanced MS column.

Table 45 - Classification of the message store IPM attributes

Message Store IPM Attribute Support				Part 1 of 2
Support by:	IPM UA		IPM MS	
Attribute	S	R	O	Comments/References
Summary Attributes:				
ipm-entry-type	M	M	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	M	

Table 45 - 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	R	O	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	
oda-1984-body-parts	–	O	O	
iso6937-body-parts	–	O	O	
bilaterally-defined-body-parts	–	O	O	
usa-privately-defined-body-parts	–	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)

Table 46 - Classification of the Pedi protocol elements

EDI Messaging Service Protocol (Pedi)					Part 1 of 6
	Support by EDI UA				
Protocol Element	S	O/R	FGs	O/R	Comments/References
InformationObject					
edim	M	M/M			
edin	M	M/M			
EDIMIdentifier					
user	M	M/M			
user-relative-identifier	M	M/M			
ExtensionField					
type	M	M/M			
criticality	M	M/M			
value	M	M/M			
EDIM					
heading	M	M/M			
body	M	M/M			
Heading					
this-EDIM	M	M/M			
originator	O	M/M			
recipients	O	M/M			
edin-receiver	O	O/M	FWD	M/M	
responsibility-forwarded	O	O/M	FWD	M/M	
edi-bodypart-type	O	M/M			
incomplete-copy	O	O/M	FWD	O/M	See Note 2
expiry-time	O	O/M			
related-messages	O	O/M			
obsoleted-EDIMs	O	O/M			
edi-application-security-elements	O	O/O	SEC-C	M/M	
cross-referencing-information	O	O/M	MBP	M/M	
edi-message-type	O	M/M			
service-string-advice	O	M/M			
syntax-identifier	O	M/M			
interchange-sender	O	M/M			
date-and-time-of-preparation	O	M/M			
application-reference	O	M/M			
heading-extensions	O	O/M			See Note 3

Table 46 - Classification of the Pedi protocol elements (continued)

EDI Messaging Service Protocol (Pedi)					Part 2 of 6
	Support by EDI UA				
Protocol Element	S	O/R	FGs	O/R	Comments/References
RecipientSubfield					
recipient	M	M/M			
action-request	O	O/M			
edi-notification-requests-field	O	M/M			
responsibility-passing-allowed	O	M/M			
interchange-recipient	O	M/M			
recipient-reference	O	M/M			
interchange-control-reference	O	M/M			
processing-priority-code	O	M/M			
acknowledgement-request	O	M/M			
communications-agreement-id	O	M/M			
test-indicator	O	M/M			
authorization-information	O	M/M			
recipient-extensions	O	O/M			See Note 3
EDINotificationRequestsFields					
edi-notification-requests	O	M/M			
edi-notification-security	O	O/O	SEC-A	M/M	
			SEC-B	M/M	
edi-reception-security	O	O/O	SEC-A	M/M	
			SEC-B	M/M	
InterchangeRecipientField					
recipient-identification	M	M/M			
identification-code-qualifier	O	M/M			
routing-address	O	M/M			
RecipientReferenceField					
recipient-reference	M	M/M			
recipient-reference-qualifier	O	M/M			
EDINReceiverField					
edin-receiver-name	M	M/M			
original-edim-identifier	O	O/M	FWD	M/M	
first-recipient	O	O/M	FWD	M/M	
RelatedMessagesField					
RelatedMessageReference	M	M/M			
edi-message-reference	O	M/M			
external-message-reference	O	M/M			
EDIApplicationSecurityElementsField					
edi-application-security-element	O	M/M			
edi-encrypted-primary-bodypart	O	M/M			
edi-application-security-extensions	O	O/M			See Note 3

Table 46 - Classification of the Pedi protocol elements (continued)

EDI Messaging Service Protocol (Pedi)					Part 3 of 6
	Support by EDI UA				
Protocol Element	S	O/R	FGs	O/R	Comments/References
CrossReferencingInformationSubfield					
application-cross-reference	M	M/M			
message-reference	O	M/M			
body-part-reference	M	M/M			
ServiceStringAdviceField					
component-data-element-separator	M	M/M			
data-element-separator	M	M/M			
decimal-notation	M	M/M			
release-indicator	O	M/M			
reserved	O	M/M			
segment-terminator	M	M/M			
SyntaxIdentifierField					
syntax-identifier	M	M/M			
syntax-version	M	M/M			
InterchangeSenderField					
sender-identification	M	M/M			
identification-code-qualifier	O	M/M			
address-for-reverse-routing	O	M/M			
AuthorizationInformationField					
authorization-information	M	M/M			
authorization-information-qualifier	O	M/M			
Body					
primary-body-part	M	M/M			
additional-body-parts	O	O/M	MBP	M/M	
PrimaryBodyPart					
edi-body-part	O	M/M			
forwarded-EDIM	O	O/M	FWD	M/M	
EDIMBodyPart					
parameters	O	O/M	FWD	M/M	
message-data	M	M/M			
MessageParameters					
delivery-time	O	O/M	FWD	M/M	See Note 1
delivery-envelope	O	O/M	FWD	M/M	See Note 1

Table 46 - Classification of the Pedi protocol elements (continued)

EDI Messaging Service Protocol (Pedi)					Part 4 of 6
	Support by EDI UA				
Protocol Element	S	O/R	FGs	O/R	Comments/References
other-parameters	O	O/O			See Note 4
MessageData					
heading	M	M/M			
body	M	M/M			
BodyOrRemoved					
primary-or-removed	M	M/M			
additional-body-parts	O	O/M	FWD	M/M	
PrimaryOrRemoved					
removed-edi-body	O	O/M			See Note 5
primary-body-part	O	M/M			
AdditionalBodyParts					
external-body-part	O	M/M			
place-holder	O	O/M			See Note 5
EDIM-ExternallyDefinedBodyPart					
body-part-reference	O	M/M			
external-body-part	M	M/M			
EDIN					
positive-notification	O	M/M			
negative-notification	O	M/M			
forwarded-notification	O	O/M	FWD	M/M	
CommonFields					
subject-edim	M	M/M			
edin-originator	M	M/M			
first-recipient	O	M/M			
notification-time	M	M/M			
notification-security-elements	O	O/O	SEC-A SEC-B SEC-C	M/M M/M M/M	See Note 8 See Note 8 See Note 8
edin-initiator	M	M/M			
notifications-extensions	O	O/M			See Note 3
SecurityElementField					
original-content	O	O/O	SEC-A SEC-B	M/M M/M	See Note 6
original-content-integrity-check	O	O/O	SEC-A SEC-B	M/M M/M	See Note 6
edi-application-security-elements	O	O/O	SEC-C	M/M	
security-extensions	O	O/M			See Note 3

Table 46 - Classification of the Pedi protocol elements (continued)

EDI Messaging Service Protocol (Pedi)					Part 5 of 6
	Support by EDI UA				
Protocol Element	S	O/R	FGs	O/R	Comments/References
PositiveNotificationFields					
pn-common-fields	M	M/M			
pn-supplementary-information	O	O/M			
pn-extensions	O	O/M			See Note 3
NegativeNotificationFields					
nn-common-fields	M	M/M			
nn-reason-code	M	M/M			
nn-supplementary-information	O	M/M			
nn-extensions	O	O/M			See Note 3
NNReasonCodeField					
nn-ua-ms-reason-code	O	M/M			
nn-user-reason-code	O	M/M			
nn-pdau-reason-code	O	O/M			
NNUAMSReasonCodeField					
nn-ua-ms-basic-code	M	M/M			
nn-ua-ms-diagnostic	O	M/M			
NNUserReasonCodeField					
nn-user-basic-code	M	M/M			
nn-user-diagnostic	O	M/M			
NNPDAUReasonCodeField					
nn-pdau-basic-code	M	M/M			
nn-pdau-diagnostic	O	M/M			
ForwardNotificationFields					
fn-common-fields	M	M/M			
forwarded-to	M	M/M			
fn-reason-code	M	M/M			
fn-supplementary-information	O	O/M	FWD	M/M	
fn-extensions	O	O/M			See Note 3
FNReasonCodeField					
fn-ua-ms-reason-code	M	O/M			See Note 7
fn-user-reason-code	O	O/M			See Note 7
fn-pdau-reason-code	O	O/M			
FNUAMSReasonCodeField					
fn-ua-ms-basic-code	M	M/M			
fn-ua-ms-diagnostic	O	M/M			
fn-security-check	O	O/O	SEC-A SEC-B	M/M M/M	

Table 46 - Classification of the Pedi protocol elements (concluded)

EDI Messaging Service Protocol (Pedi)					Part 6 of 6
Support by EDI					
Protocol Element	S	UA O/R	FGs	O/R	Comments/References
FNUserReasonCodeField					
fn-user-basic-code	M	M/M			
fn-user-diagnostic	O	O/M	FWD	M/M	
FNPDAUReasonCodeField					
fn-pdau-basic-code	M	M/M			
fn-pdau-diagnostic	O	M/M			

Notes

1 M on origination if the implementation supports forwarding of a multi part EDIM without accepting responsibility.

2 Mandatory (on origination) when an implementation supports the removal of body parts.

3 Critical extensions must be supported in order to accept responsibility.

4 Use of supplementary information fields requires bilateral agreement.

5 Mandatory on origination if removal of body parts is supported.

6 One of these two elements must be supported on origination when using the SEC-A or SEC-B EDI security class.

7 One of these two elements must be supported on origination.

8 M on origination if EDI-notification-security or EDI-reception-security (of the EDINotificationRequestsFields) are supported on reception.

A.12 Message store EDIMS attribute support

A.13 Classification of the P3 protocol elements for physical delivery

The protocol elements used in Table 48 should be viewed as a delta to the kernel as classified in Table 34. Thus, Table 48 shows the additional supported required in P3 to conform to the Physical Delivery functional group.

Table 48 - Classification of the P3 protocol elements for physical delivery

MTS Access Protocol (P3) for Physical Delivery					Part 1 of 1
Static Support by:	UA	MS	MTA		
Protocol Element	O/R	O/R	O/R	Dyn	Comments/References
MessageSubmissionEnvelope					
extensions					
originator-return-address	M/-	M/-	-/M		
PerRecipientMessageSubmission Fields					
extensions					
physical-forwarding-prohibited	M/-	M/-	-/M		
certification-path	M/-	M/-	-/M		
ORName					
extension-attributes					
physical-delivery-country-name	M/-	M/-	-/M		
postal-code	M/-	M/-	-/M		
unformatted-postal-code	M/-	M/-	-/M		

Annex B (normative)

Object identifiers

B.1 X.400 SIG object identifiers

The X.400 SIG object identifiers all allocated under the *mhsig* node in the OIW object identifier subtree, as defined in part 6 of the Stable Implementors Agreements document. This definition is duplicated in figure 15.

```
id-mhsig  OBJECT IDENTIFIER  ::=
            { iso (1)  identified-organization (3)  oiw (14)  mhsig (6) }
```

Figure 15 - Definition of the *mhsig* object identifier

The X.400 SIG has defined several categories of object identifiers. Their definition is provided in figure 16.

```
id-mhsig-content-types    OBJECT IDENTIFIER  ::=
                            { id-mhsig  content-types (0)  }

id-mhsig-body-part-types  OBJECT IDENTIFIER  ::=
                            { id-mhsig  body-part-types (1)  }
```

Figure 16 - Defintion of the X.400 SIG Object Identifier Categories.

B.2 Content types

There are presently no object identifiers for content types allocated by the X.400 SIG.

B.3 Body part types

The object identifiers for the external body part types allocated by the X.400 SIG are defined in figure 17.

```
id-privacy-enhanced-mail  OBJECT IDENTIFIER  ::=
                            { id-mhsig-body-part-types  pem (0) }
```

Figure 17 - Definition of the External body part object identifiers

B.4 Security classes

The ASN.1 expressed in figure 18 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 18 - 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 10), the originator of the forwarding message shall set the original encoded information types in the P1 envelope to Undefined 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 49 are covered by the category "other."

Table 49 - 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 48 and the algorithm in figure 19 should be used.

```
IF current character is in the encoding set THEN
  encode the character according to table 48
ELSE
  write the current character;
continue reading;
```

Figure 19 - ASCII to PrintableString algorithm

To decode a PrintableString representation to an ASCII representation, table 48 and the algorithm in figure 20 should be used.

```
IF current character is not "(" THEN
  write character
ELSE
  {
  look ahead appropriate characters;
  IF composite characters are in table 48 THEN
     decode per table 48
  ELSE
  write current character;
  }
continue reading;
```

Figure 20 - PrintableString to ASCII algorithm

D.2 Rendition of IA5Text

The characters that may be used in an IA5String are the graphic characters (including Space), control characters and Delete of the IA5 character repertoire ISO 646.

The graphic characters that may be used with a guaranteed rendition are those related with positions 2/0 to 2/2, 2/5 to 3/15, 4/1 to 5/10, 5/15 and 6/1 to 7/10 in the basic 7-bit code table.

The other graphic characters may be used but have no guaranteed rendition.

The control characters that may be used but have no guaranteed effect are a subset consisting of the format effectors 0/10 (LF), 0/12 (FF) and 0/13 (CR) provided they are used in one of the following combinations as defined in table 50.

Table 50 - Interpretation of format effector combinations

Combination	Interpretation
CR LF	to start a new line
CR FF	to start a new page (and line)
LF .. LF	to show empty lines (always after one of the preceding combinations).

The other control characters or the above control characters in different combinations may be used but have no guaranteed effect.

The character Delete may occur but has no guaranteed effect. The IA5String in a P2 IA5Text BodyPart represents a series of lines which may be divided into pages. Each line should contain from 0 to 80 graphic characters for guaranteed rendition. Longer lines may be arbitrarily broken for rendition.

> **NOTE -** X.408 states that for conversion from IA5Text to Teletex, the maximum line length is 77 characters.

D.3 EDI use of MHS

D.3.1 P0 recommended practice

This section outlines a recommended method for interworking between a P(edi) UA with a UA implementing the Recommended Practice (EDI Use of X.400) in parts 7 and 8 of the OIW Stable Implementation Agreements. That Recommended Practice is commonly referred to as the "P0" approach to EDI use of the X.400 MTS.

This section does not define where the conversion between the two content types occurs. It is possible for the conversion to be performed by the P0 UA, the P(edi) UA, or a gateway. The Recommended Practice outlined in this section only attempts to document the rules that should be followed to ensure a conversion which retains the maximum amount of information.

D.3.1.1 P0 to P(edi) conversion

The converting entity may assume that the P0 content contains only one EDI interchange. This interchange will become the first and only body part of the EDIM.

The content type field of the message will have the value "undefined" before the conversion and will have the integer value "35" or the object identifier value for P(edi) which is specified in X.435 after conversion. The EDIM Heading fields can be formed using the following rules:

EDIMIdentifier: Originator ORName concatenated with the UTCTime at which the conversion from P0 to P(edi) was performed.

Originator: Originator ORName.

Recipients: Recipients from the P1 envelope. EDI Notification Requests are not specified as none are requested when using the P0 approach.

EDIBodyPartType: This element may have one of deveral values depending on the encoded information type (EIT) value of the P0 message or the ability of the converting entity to determine which EDI syntax is present in the content:

a) X.435-defined value for ANSI X12/EBCDIC if the EIT field of the P1 envelope has the value "undefined".

b) X.435-defined value for ANSI X12/ISO 646 if the EIT field of the P1 envelope has the value "IA5String".

c) Any other valid value if the entity performing the conversion can determine which EDI syntax is contained in the content and which character encoding is used for the EDI syntax.

Other heading fields will only be set if the entity performing the conversion is capable of parsing the EDI Interchange and discovering the correct values of EDI Heading fields.

As the P0 message will not contain requests for EDI Notifications, an EDI UA will never create an EDIN when it receives an EDIM converted from P0 .

D.3.1.2 P(edi) to P0 conversion

When converting a P(edi) content to a P0 content, the following rules apply:

The first body part of the EDIM will be copied to the content. **All other body parts of the EDIM will be discarded.**

The P1 envelope fields shall have the following values:

Content Type: Value for "undefined".

Originator: Originator ORName.

Recipients: Recipients from the EDIM Heading. An NN EDIN with NN Reason Code set to the value "unspecified" is created for each Recipient for whom a Notification Request was specified. The EDIN Originator is set to the Recipient ORName. It is recommended that the supplementary information field of the NN be used to provide additional information on the disposition of the EDIM.

Encoded Information Types (EITs): This element may have one of several values depending on the value of the EDI Body Part Type:

a) The EIT is set to "undefined" if the EDI Body Part Type is encoded with the EBCDIC character set.

b) The EIT is set to "IA5String" if the EDI Body Part Type is encoded using the ISO 646 (ASCII) character set.

c) A value is not present for the EIT if EDI Body Part Type does not contain one of the above mentioned values.

D.3.2 P2 recommended practice

As there are a substantial number of users in the NIST OIW community that implemented the CEC TEDIS "P2" approach to EDI use of the X.400 MTS, this section will also include text that describes interworking between a P(edi) UA and a P2 UA. This text is not maintained by the EDI Working Group of the NIST OIW X.400 SIG but is included for the convenience of our user community. Users intending to interwork between P2 and P(edi) User Agents should consult the current version of the EWOS/ETSI document "A/3331 - Functional Profile of an Electronic Data Interchange User Agent." This will ensure that the most up to date technical information is obtained.

D.3.2.1 Conversion from IPMS to EDIMS (P2 to P(edi))

It is assumed that there is one and only one body part in the IPM Message, and that this body part contains an EDI interchange.

The IPM becomes the first, and only, body part of the EDIM.

The EDIM Heading fields are set as follows:

EDIMIdentifier: Originator ORName concatenated with the LocalIPMIdentifier portion of the IPM Identifier.

Originator: Originator ORName.

Recipients: Recipient ORNames from the IPM Heading. The edi-notification-requests-field is not coded.

EDIBodyPartType: The value is a local implementation issue. If the entity performing the conversion can identify the EDI syntax of the EDI Interchange then it can specify an appropriate value. Otherwise, the entity must be assuming a specific encoding and will specify the value for the syntax it is assuming.

Other heading fields may be set if the entity performing the conversion is capable of parsing the EDI Interchange and discovering the correct values of the EDIM Heading fields.

Since there are not notification requests, the EDI UA will never create an EDIN when it receives a converted EDIM and therefore the action for handling EDINs in the reverse direction does not need to be considered.

D.3.2.2 Conversion from EDIMS to IPMS (P(edi) to P2)

> **NOTE -** The verification of authority to perform a particular conversion is outside the scope of this annex. It is assumed that such conversion will be done with the full knowledge of the originating and recipient parties.

The EDIBodyPart of the EDIM will be copied to the IPM body as an IA5TextBodyPart. All other body parts of the EDIM will be discarded.

The IPM Heading fields are set as follows:

IPM Identifier: EDIMIdentifier.

Originator: Originator ORName.

Recipients: Recipients from the EDIM Heading. All recipients become IPM Primary Recipients. An NN EDIN with NN Reason Code set to the value "unspecified" is created for each Recipient for whom a Notification Request was specified. The EDIN Originator is set to the Recipient ORName. The EDIN Originator is set to the Recipient ORName. IPM Notifications shall not be requested.

Subject: Not present or set to a single blank character.

If EDINs have been requested the originator will always receive an NN. Since no IPM notifications are requested, the IPM UA will never create an IPM notification when it receives an IPM converted from an EDIM and therefore handling of notifications in the reverse direction does not need to be considered and is not an option for generating EDINs.

D.4 ODA transfer

To ease interworking with 1984 implementations when transferring Office Document Architecture (ODA) documents, the following are recommended for 1988 implementations:

a) Origination UA implementing 1988 Implementation Agreements. The 1988 will generate the ODA according to CCITT Recommendation T.411 Annex E for the destination UA(s) implementing 1988 Implementation Agreements. If the destination UA supports 1984 Implementation Agreements, the approach as described in section 7.12.8 is recommended.

b) Recipient UA implementing 1988 Implementation Agreements. The recipient system will be able to handle the ODA bodypart in P2 (1984) as defined in part 7, B.8.1 for interworking with 1984 implementation, and will also be able to handle the ODA bodypart as defined in the appropriate base standards.

c) MTA downgrading rules. When transferring an P22 with ODA body part in P22 as described in T.411 to an 1984 MTA, the EITs identified by ODA Object Identifiers are mapped to bits 0 and 10 of the built-in EITs.

If the UA does not register to support P22 or ODA bodypart, a Non-Delivery-Report will be generated as required.

D.5 Use of externally defined body part

D.5.1 General

An Externally Defined body part represents an information object whose semantics and abstract syntax are denoted by an Object Identifier which the body part carries. This body part type enables the exchantge of information objects of all kinds, each unambiguously and uniquely identified.

The Externally Defined Body Part definition is reproduced in figure 22.

```
ExternallyDefinedBodyPart   ::= SEQUENCE {
  parameters                     [0] ExternallyDefinedParameters  OPTIONAL,
  data                               ExternallyDefinedData  }

ExternallyDefinedParameters ::= EXTERNAL
ExternallyDefinedData       ::= EXTERNAL

EXTERNAL                    ::= [UNIVERSAL 8]  IMPLICIT SEQUENCE  {
  direct-reference              OBJECT IDENTIFIER  OPTIONAL,
  indirect-reference            INTEGER  OPTIONAL,
  data-value-descriptor         ObjectDescriptor  OPTIONAL,
  encoding                      CHOICE  {
    single-ASN1-type              [0]  ANY,
    octet-aligned                 [1]  IMPLICIT OCTET STRING,
    arbitrary                     [2]  IMPLICIT BIT STRING  }  }

    Note -  In the case of transfer of EXTERNAL in P2 BodyPart, the
    direct-reference component is mandatory and the indirect-reference and
    data-value-descriptor components must be absent.
```

Figure 22 - Externally Defined body part definition

On the basis of the Externally Defined body part type, all body part types are divided into two important classes as follows:

a) *basic:* Said of any body part type except Externally Defined. All basic body part types are denoted by an integer (an ASN.1 context-specific tag) and are defined in section 7.3 of X.420.

b) *extended:* Said of the Externally Defined body part type restricted to any one value of the Direct-reference component of the Data component of such a body part. Denoted by an Object Identifier.

Annex B of Recommendation X.420 defines some (but not necessarily all) extended body part types.

D.5.2 Use of equivalents of basic body part types

For each basic body part types, section B.1 of Recommendation X.420 defines an equivalent extended body part type. In order to facilitate interworking with 1984 systems, use of these extended body part types is not recommended; the basic body part types should be used instead.

Editor's Note: The requirements of this clause may change when interworking with 1984 systems is no longer critical.

D.5.3 Use of General Text body part type

Unless otherwise specified in these agreements (e.g., IA5Text, 6937Text, Teletex) the General Text body part as defined in ISO 10021-7 Annex B.2 is the preferred means of supporting unstructured text body parts. The character set registration referred to in that annex is provided by ECMA.

D.5.4 Use of File Transfer body part type

The File Transfer body part type is the recommended mechanism for the exchange of complex computer data via intra- and inter-company X.400 messages. It enables automatic type recognition for the file being sent and, possibly, automatic invocation of the appropriate application necessary to process the data.

D.5.4.1 Encoding of General Identifier

In order to optimize the machine-processing of information encoded in the Parameters and to enable registration, it is recommended that, if present, General Identifiers should be encoded as Object Identifiers.

D.5.4.2 Encoding of Contents Type

It is recommended that the Contents Type parameter be encoded as document type. The encoding as constraint-set-and-abstract-syntax has been provided only for backward compatibility with FTAM and its use is discouraged.

D.5.4.3 Encoding of application specific information

The type of a file can be considered from several perspectives:

a) As a specific data structure consisting of a sequence of presentation data values - the position taken by the FTAM standard;

b) As the output of a certain application - the position taken by e-mail users requiring the interchange of office documents.

The fact that registered OSI document types have to be recognized by FTAM implementations and be described according to the requirements of ISO/IEC 9834-2 "Registration procedures for OSI document types" makes use of the Contents Type parameter inappropriate for expressing point of view (b).

Considering that the environment parameter "application-reference" could describe not only the application that generated a document but, more generally, the application-level format of the document, it is recommended that the values given to the "application-reference" parameter component be Object Identifiers associated with such a format.

Example: If an Object Identifier has been associated with a certain word-processing file format then this Object Identifier should be used as the value of "application-reference" when a file of that format is carried by a File Transfer body part, while the Content Type parameter should have as its value the Object Identifier associated with the "unstrucutred-binary" document type.

D.5.4.4 EITs for the File Transfer body part

It is recommended to use only the id-eit-file-transfer Object Identifier in association with the File Transfer body part.

The use of EITs describing other parameters of the File Transfer body part such as contents types, application references, etc. would force all potential recipients to register a possibly large number of EITs in order to avoid non-delivery of messages.

D.5.5 Use of other extended body part types

The following are guidelines regarding the use of Externally Defined body part types not defined in the X.400 or other standards:

a) *Use of Parameters component:* In simple cases, to ease the integration of applications to X.400 systems, the Parameters component need not be used.

b) *Use of Data component:* For each different format of data, different Object Identifiers for the Data component are recommended. If an application chooses to use ASN.1 to format the data to achieve a single representation across platforms, the single-ASN1-type encoding choice should be used. Otherwise:

1) The octet- (i.e., byte) aligned choice is used if the data format is octet-aligned; or,

2) The arbitrary choice is used if the data is bit-aligned.

c) *Assignment of Object Identifiers:* Object Identifiers need to be assigned for the EXTERNALs, and these identifiers for the Parameters and Data components should be different. The Object Identifier for an EXTERNAL also indicates the syntax of the data encoding, i.e., whether single-ASN1-type or octet-aligned or bit-aligned is being used.

NOTE - Use of proprietary Externally Defined body part types is recommended only if the extended body part types already defined in the standards do not provide the apporpriate functionality.

In order to communicate with 1984 systems, the use of the Bilaterally Defined body part is recommended.

D.5.6 Obtaining object identifiers

There are many ways to obtain object identifiers. One such way is described as follows:

a) The application provider obtains a unique Numeric Name form for their organization from ANSI, as described in ANSI ISSB 840 and ISSB 843, and appends this number form to {iso (1) member-body (2) US (840)} to form an object identifier denoting their organization.

b) The application provider (organization) allocates a series of numbers to identify the application data format; these numbers are appended to the object identifier constructed in step (i) to form an object identifier that is globally unique. It is recommended that the application provider (organization) use a hierarchical structure for identifying their data types to ease the administration of the identifiers.

For example, company PCSoftware Inc. obtains the organization number "999" from ANSI. The PCSoftware SpreadSheet file for MS-DOS might be assigned the following object identifier.

NOTE - ASN.1 notation is used. The numbers in parentheses form the identifier, the associated words describe the number.

{ iso (1) member-body (2) US (840) PCSoftware Inc. (999) MS-DOS-Application (1) SpreadSheet (3) Data (1) }

D.6 Privacy Enchanced Mail body part

This clause describes a mechanism to convey an Internet Privacy Enhanced Mail (PEM) message across an X.400 MHS. PEM is described in Internet RFCs 1113, 1114, and 1115 and their successors.

The general Internet mail message format is described in RFC 822. Mapping of RFC 822 messages to and from X.400 Inter Personal Messages is described in RFC 987 for 1984 X.400 and in RFC 1148 for 1988 X.400.

The PEM message is conveyed as a P2(2) body part. All of the RFC 822 header information is conveyed in the P1 envelope and P2 header per RFC 987 and RFC 1148. The PEM message (encapsulated security header and, possibly encrypted, message text as described in RFC 1113) is conveyed in a single body part. On the X.400 side, this body part may be manipulated like any other body part; e.g., it may be included in a multi-part body.

For 1988 (P22), the PEM body part is externally defined and does not require parameters. This definition is provided in figure 23.

```
privacy-enhanced-mail      EXTENDED-BODY-PART-TYPE
                             DATA  OCTET STRING
                      ::=  id-privacy-enhanced-mail

-- The object identifier is defined in annex B.
```

Figure 23 - Definition of the Privacy Enhanced Mail body part type

For interworking with 1984 (P2) systems, a USA body part (integer) will be allocated by NIST as described in figure 10.

D.7 Selection of OR name attributes

To support the transition to addresses with Teletex components, it is recommended that a printable string alternative address be established for each address containing Teletex strings.

D.8 Use of the Teletex body part

The Teletex body part should be used purely for structured teletex documents, as described in F.200 and T.60, obeying page rules, etc. It should not be used to transfer T.61 characters, in a general sense, across the MTS. If only IA5 characters are being used, the IA5Text body part should be used, especially when interworking with 1984 UAs is relevant. Otherwise, the GeneralText body part should be used to transfer unstructured character data.

D.9 Provision of security class S0A using asymmetric algorithms

This clause describes one method of providing the security services of class S0A when using asymmetric (public key) cryptographic algorithms. It is recommended that this method be used unless the security requirements or policy specifies otherwise. Asymmetric cryptographic algorithms such as RSA are used to provide digital signatures in support of the content integrity and (end-to-end) message origin authentication services, as well as proof of delivery. Since asymmetric algorithms are used, the non repudiation of origin and non repudiation of delivery services of security class S2 are also provided. Content confidentiality is provided using a combination of symmetric and asymmetric encryption. The following paragraphs discuss the protocol elements used to provide these services, as well as certificate management and other issues.

D.9.1 Protocol elements

The following protocol elements are provided by the originating UA in the submission envelope in support of the S0A security services.

Content: If the content confidentiality services is required, the message content is encrypted under the content confidentiality key.

Content Integrity Check: This per-recipient security element is a signature over the message content, and provides the content integrity, message origin authentication, and non repudiation of origin services if content confidentiality is not required. (If the message is encrypted, the content integrity check is included in the message token.)

> **NOTE -** The message origin authentication check provides a single signature, rather than a signature per recipient, thus reducing total message size in the case where multiple recipients are present. However, support for this protocol element is optional for security class S0. In addition, it is computed over the message content as sent (i.e., the encrypted content if content confidentiality is used). If the content is encrypted, this protocol element does not truly provide non repudiation of the unencrypted content. In this case, smaller message size was traded off for the additional service of non repudiation.

Proof Of Delivery Request: This per-recipient security element is used to request the recipient to generate a proof of delivery, in the case where content confidentiality is not used. (Where content confidentiality is used, the proof of delivery request is included in the message token, as shown below.)

Originator Certificate: This security element is a set of one or more certificates which the recipient may use to obtain the originator's public key. For example, it might contain the chain of certificates from the originator, through the certification hierarchy to a top-level certification authority.

Message Token: The asymmetric message token conveys security information from an originator to a single recipient. It is a signed structure, some of whose fields may be encrypted. The message token is used only when content confidentiality is desired, and supports the content integrity, message origin authentication, content confidentiality, and non repudiation of origin services. The following fields are required, and all other fields are optional:

- *Signature Algorithm Identifier:* The algorithm identifier of the asymmetric algorithm used to sign the token.

- *Recipient Name:* The OR Address and/or Directory Name of the recipient with whom the token is associated. Since the encrypted portion of the token is encrypted under the recipient's public key, it is recommended that the directory name be included, since the recipient's certificate contains his/her directory name rather than OR Address.

- *Time:* The time of day when the token was generated.

- *Signed Data:* The following fields are signed but not encrypted:

a) *Content Confidentiality Algorithm Identifier:* The algorithm to be used to encrypt the message content.

b) *Proof of Delivery Request:* This element is used to request the recipient to compute a proof of delivery over the received message.

- *Encrypted Data:* These fields are encrypted under the recipient's public key:

c) *Content Confidentiality Key:* The symmetric key used to encrypt the message content.

d) *Content Integrity Check:* A signature on the unencrypted message content. If content confidentiality <u>is</u> required, this element provides the content integrity, message origin authentication, and non repudiation of origin services. This signature is encrypted in order to protect against the "low entropy" attack described in Internet RFC 1113. (In RFC 1113, the signature is encrypted under the content confidentiality key.)

NOTE - The encrypted portion of the token will then comprise two RSA encryption blocks.

The following element of service is generated by the recipient, if requested by the originator.

Proof Of Delivery: This security element provides proof and non repudiation of delivery. It is a digital signature computed over the received (possibly encrypted) message content and various delivery envelope fields, as defined in the base standard.

D.9.2 Algorithm selection

This clause makes no recommendation as to hash algorithms, asymmetric encryption algorithms, or symmetric encryption algorithms. The implementor must select appropriate algorithms, based on factors such as performance, cost, and licensing and export restrictions. A fairly complete list of algorithms can be found in clause 7 (Security Algorithms) of Part 12 of these Agreements. In some cases, the implementor must also specify certain algorithm-dependent information. For example, when using the symmetric algorithm **DES-CBC**, the implementor must specify the padding mechanism used, since this algorithm operates on 8-byte input blocks. Internet RFC 1115 defines such padding rules for DES and RSA in various modes, and these mechanisms are recommended unless security requirements dictate otherwise. PKCS #1 (see Bibliography, Annex F) discusses such matters in more detail.

D.9.3 Certificate management

Management of public key certificates is beyond the scope of this recommended practice. X.509 provides a generic authentication framework which uses the Directory to store certificates. In the absence of a ubiquitous Directory, local means may be used to obtain certificates. For example, the recipient of a message might choose to cache those certificates received in the **OriginatorCertificate** protocol element of the delivery envelope.

Each community of interest will define its own policy regarding certificate management and the associated trust model. An example of a centralized trust model can be found in Internet RFC 1114, while the most complete example of a decentralized trust model can be found in the paper on Digital's Distributed System Security Architecture cited in the Bibliography (Annex F).

D.9.4 Other issues

In the case of the P2 content type, addressing information may be protected by replicating the P1/P3 recipient names in the P2 heading fields (To:, CC:, and BCC:). The X.400 security services discussed above are applied to the entire P2 IPM, including the heading and all body parts. Additional protection of heading and envelope fields may be provided using double enveloping.

When using X.400 (1988) distribution lists (DLs), one might choose to distribute the private key associated with the DL to all members of the DL. This allows an originator to create a single message token in which the content confidentiality key is encrypted under the DL's public key. (This requires support of the DL expansion history protocol element on delivery, so that the recipient may select the proper private key for decryption. Alternatively, the originating UA may expand the DL locally and generate a message token for each member (recursively). There is no architected support for this mechanism in the base standard, nor is there architected support for performance of this function by an MTA when expanding a DL.

Annex E (informative)

Secure messaging guidelines

E.1 Introduction

The purpose of the security functional group is to define an approach to the provision of secure messaging with Message Handling systems within the general framework of these Implementation Agreements.

E.2 Message handling vulnerabilities

The message handling vulnerabilities (threats) which can be protected using security measures are defined in Annex D (Security Threats) to Recommendation X.402 (1988):

a) Masquerading;

b) Message sequencing;

c) Modification of information;

d) Denial of service;

e) Repudiation;

f) Leakage of information.

Other specific threats exist if there is a failure to maintain information separation, which includes:

a) Manipulation;

b) Misrouting.

Some of these threats are defined in ISO standard IS 7498, OSI Reference Model, Part 2: Security Architecture. The ISO standard also specifies other threats, not all of which are relevant to message handling systems.

Annex D to CCITT Recommendation X.402 (1988) also indicates which MHS security services may provide protection against such threats.

Some threats to message handling systems cannot be easily prevented, merely detected, others are not appropriated for standardization.

E.3 General principles

E.3.1 Security policy

A general security policy can be defined as the set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information. Thus a security policy defines an organization's overall approach to security and must cover all security aspects.

Security within an organization is not only the concern of message handling service and must be viewed in a more global and general sense. The wider aspects of a security policy would therefore include personnel security (such as the vesting and confidence placed in staff), end-user access control, physical, procedural and documentation security. These Implementation Agreements however are only concerned with Electronic Information Security (EIS), specifically in the areas of communications (COMSEC) and computer (COMPUSEC) as applicable to standardization of a secure message handling system operating in a store and forward environment.

E.3.2 Security classes

In the X.400 (1988) Recommendations, some threats are countered by EIS measures, these measures are realized by providing security services and implemented using security elements.

These Implementation Agreements groups together security features of a message handling system defined by the base standards into separate 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.

These Implementation Agreements includes a set of security classes; each class stipulates a set of mandatory and optional security services. The security classes are incremental subsets of the security features in the MHS Base Specifications:

> *Security Class S0* only requires support of end-to-end security services between UAs (content integrity, message origin authentication, proof of delivery), and hence can be used to provide some protection even in the case of transit through an intermediary MTS which may not be trusted.
>
> *Security Class S1* additionally requires support and use of secure access management within the MTS so as to allow the enforcement of a label-based security policy and enable trusted interworking between security domains.
>
> *Security Class S2* additionally requires support and use of origin authentication checks within the MTS to verify the origin of messages, probes, and reports, thereby making it possible to provide non-repudiation within the MTS.

Mandatory security services within a security class can be selected by the subscriber or user, either on a per-message basis, or for an agreed contractual period of time. It is a local issue to determine when a mandatory security service is offered for user selection or when it is permanently invoked. Facilities and mechanisms to support the mandatory security services must always be provided within the security class, which specifies the services as "mandatory."

E.3.3 Dynamic behavior requirements

The use of some security services is always required for certain security classes. This is specified in these Implementation Agreements by imposing additional dynamic requirements, to those specified in the base standards, ensuring that the corresponding protocol elements are always present.

Similarly, use of some security services are prohibited for certain security classes. This is specified in these Implementation Agreements by imposing additional dynamic requirements to those specified in the base standards, ensuring that the protocol elements are never present.

E.3.4 Encryption techniques

The secure messaging facilities defined in the base standards are provided using three basic security techniques, namely:

a) Symmetric encryption;

b) Asymmetric encryption;

c) Trusted functionality (i.e., COMPUSEC measures).

The base standards permit the use of the techniques on an individual basis to provided security services or they can be combined in support of a security policy. These Implementation Agreements combine the techniques in order to provide a comprehensive set of security facilities, which are intended to counter various combinations of the vulnerabilities of a messaging service. In some cases the security services defined in the base standards can only be implemented using one of the techniques above, namely asymmetric encryption. However, the actual technique employed shall be dependent on the algorithms, which shall be registered by a security authority for the domain.

It is the intention of these Implementation Agreements that implementations will not be restricted to asymmetric techniques. All the mandatory security services can be implemented using trusted functionality in combination with symmetric, asymmetric, or both encryption techniques.

Although the base standards defines the syntax of an asymmetric token, these Implementation Agreements takes into account the ISO/CCITT MHS Implementors' Guide, which permits the use of both asymmetric and symmetric techniques for both the signed and encrypted data.

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.

E.3.5 Implementation considerations

E.3.5.1 Peer 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.

E.3.5.2 Confidentiality

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.

E.3.5.3 Integrity

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.

E.3.5.4 Message 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.

E.3.5.5 Non-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-repudication 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.

E.3.5.6 Secure 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).

E.3.5.7 Implications 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.

E.3.5.8 Implications 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).

E.3.5.9 Implications 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.

E.3.5.10 Implications 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.

E.3.5.11 Implications 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.

E.3.5.12 Accountability

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.

E.3.5.13 Double 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 24 illustrates the technique.

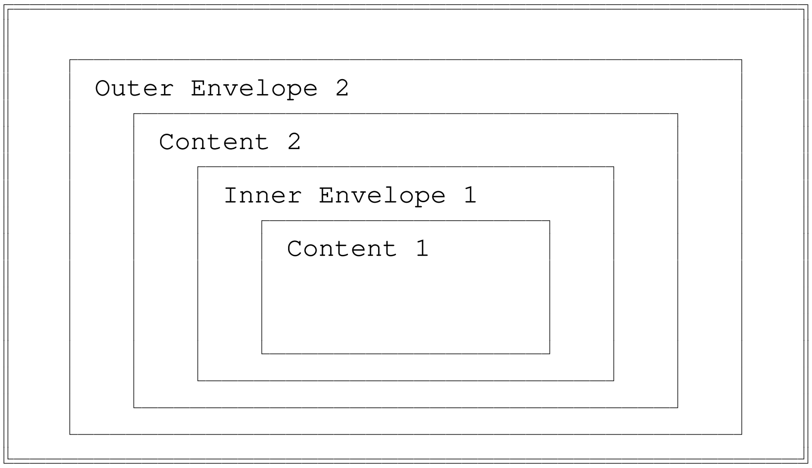

Figure 24 - Double enveloping technique

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.

E.4 Security class S0

E.4.1 Rationale

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.

E.4.2 Technical 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; and,

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

E.5 Security class S1

E.5.1 Rationale

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.

E.5.2 Technical 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.

E.6 Security class S2

E.6.1 Rationale

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.

E.6.2 Technical 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.

E.7 Confidential security class variants (S0a, S1a, and S2a)

E.7.1 Rationale

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.

E.7.2 Technical 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 F (informative)

Bibliography

F.1 ANSI

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 U. S. Register is included.

F.2 Internet

Message Encipherment and Authentication Procedures, RFC 1113.

Certificate-based Key Management, RFC 1114.

Algorithms, Modes, and Identifiers, RFC 1115.

Annex G (informative)

Defense message handling profiles

G.1 Introduction

Several additional requirements for Message Handling Systems (MHS) in the U.S. Department of Defense (DoD) are currently being investigated by the Data Communications Protocol Standards (DCPS) Technical Management Panel (DTMP). This annex describes the DoD Standardized Profile(s) (DSP) that are required for Defense Message System (DMS) use.

Two multipart DoD profiles are currently defined, namely:

- DSP AMH1n(D) - Information Technology - Defense Standardized Profiles AMH1n(D) - Message Handling Systems - Common DoD Messaging

- DSP AMH2n(D) - Information Technology - Defense Standardized Profiles AMH1n(D) - Message Handling Systems - Military Messaging

These profiles will be published as part of the MIL-STD-2045 series. The AMH1n(D) profile consists of a DoD delta to the AMH1n ISP. AMH2n(D) is a standalone profile of a new military messaging content type (P772) based on the IPM content type. These extensions support military-unique functionality required by the DMS.

For further information on these profiles, contact:

DTMP WG/2 Chairman
c/o Defense Information Systems Agency (DISA)
Joint Interoperability Engineering Office (JIEO)
Code TBBD
Fort Monmouth, NJ 07703-5000
Phone: 908-532-7726

Annex H (informative)

Differences between OIW Agreements and EWOS/ETSI Draft Profile A/3312

H.1 P7

The "and," "or," and "not" elements of Filter are optional in A/3312.

The "equal," "greater-or-equal," "less-or-equal," and "present" elements of FilterItem are optional in A/3312; however, at least one must be implemented.

The List and Summarize operations are optional for the UA Kernel in A/3312.

The "precise" element in the Fetch operation is optional for the UA Kernel in A/3312.

Index