Stable Implementation Agreements for Open Systems Interconnection Protocols: Part 29 - Common Messaging ISP

Output from the December 1993 NIST Workshop for Implementors of OSI

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

Foreword

The text in this chapter contains the draft working text for MHS ISP AMH1n on Common Messaging, and related supporting documents. It is retained here as a temporary placeholder until promulgation of the ISP is completed. The ISP is included in its final DISP editorial form, without additional OIW specific notation. The following documents are contained in this chapter:

- Explanatory Report for Parts 1-5 of pDISP 10611 - Message Handling Systems - Common Messaging
- ISP 10611-1: MHS Service Support
- ISP 10611-2: Specification of ROSE, RTSE, ACSE, Presentation and Session Protocols for use by MHS
- ISP 10611-3: AMH11 - Message Transfer (P1)
- ISP 10611-4: AMH12 - MTS Access (P3)
- ISP 10611-5: AMH13 - MS Access (P7)
- Editorial Errata - ISO/IEC DISP 10611 (AMH1)
- Editor’s Comments on ISO/IEC DISP 10611-5 (AMH13)

From: EWOS

To: ISO/IEC JTC1/SGFS

cc: OIW
AOW

Date: 1993-2-25

Subject: **pDISP 10611 - Message Handling Systems - Common Messaging**

The enclosed Explanatory Report and the 5 parts of pDISP 10611 are herewith submitted to ISO/IEC JTC1/SGFS for formal review and processing for DISP ballot.

All outstanding issues were resolved at the 6th MHS ISP Special Group (MISG) meeting (Kyoto, Japan, February 1-4, 1993), and the pDISPs have been approved for SGFS submission by the three regional workshops.

SGFS are also requested to consider the continuing requirement for public and timely visibility of the explanatory material relating to the structure of the ISP and the profiles contained therein, as included in clauses D and F of the Explanatory Report. Similar material was submitted to SGFS in early 1992 for inclusion in the SGFS N100 directory but, with the revision in scope and nature of that directory (as the new standing document SD-4), it is no longer evident where such material should be located. One possibility is to include it as a introductory part to the ISP itself. However, it is the opinion of the MISG that explanatory material of this nature is an important requirement for potential users of ISPs (both suppliers and purchasers) and should therefore ideally be obtainable separately (and hence separately identified in the ISO catalogue) and, if possible, in advance of final publication of the ISP.

J B Stranger

Editor, pDISP 10611

TITLE: **Explanatory Report for Parts 1-5 of pDISP 10611 - Message Handling Systems - Common Messaging**

SOURCE: EWOS

DATE: 1993-2-25

STATUS: Final version for submission to ISO/IEC JTC1/SGFS together with pDISP 10611

This explanatory report has been prepared in accordance with ISO/IEC JTC1/SGFS SD-1 (SGFS N601, 1992-08-24) which specifies the taxonomy update, ISP approval and maintenance process.

A. General Profile Information

1. *Profile identification*

These parts of pDISP 10611 cover the profiles with taxonomy identifiers AMH1n, as listed in clause 6.3.2 of ISO/IEC TR 10000-2 : 1992 and as follows:

AMH11 - Message Transfer (P1)
AMH12 - MTS Access (P3)
AMH13 - MS Access (P7)

Profile AMH11 is further subdivided into AMH111 (Normal mode) and AMH112 (X.410(1984) mode).

2. *Submitting organization and contact point*

The submitting organization is:

European Workshop for Open Systems
Rue de Stassart 36
B-1050 Brussels
Belgium

Tel: +32 2 511 7455
Fax: +32 2 511 8723

The editor for all parts of this submission who will serve as contact point during the review and approval process is:

J B Stranger
Information Strategies Limited
22 Walford Road
LONDON N16 8ED
UK

Tel: +44 71 254 5130
Fax: +44 71 923 1466

3. *Date of original notification to SGFS*

Submission of harmonized taxonomy update - 1992-4-23

Notice of intent to submit draft pDISP 10611 for informal quality review - 1992-7-11

Submission of draft pDISP 10611 for informal quality review - 1992-8-12

4. *Declaration of commitment to maintain*

On behalf of the three regional OSI/OSE workshops, EWOS undertakes to ensure that these parts of pDISP 10611 will be maintained. The contact point for maintenance is the Chairman of EWOS EG MHS, who can be contacted via the EWOS secretariat at the above address.

B. Base Standards Referenced

1. *ISO/IEC standards, technical reports and CCITT recommendations referenced*

References listed without a publication date are expected to be published during 1993.

ISO 7498-2: 1990*, Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture.*

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

ISO/IEC 9066-2: 1989*, Information processing systems - Text Communication - Reliable Transfer - Part 2: Protocol specification.*

ISO/IEC 9072-2: 1989*, Information processing systems - Text Communication - Remote Operations - Part 2: Protocol specification.*

ISO/IEC 9594-8: 1990*, Information technology - The Directory - Part 8: Authentication framework. [see also CCITT Recommendation X.509(1988)]*

ISO/IEC TR 10000-1: 1992*, Information technology - Framework and taxonomy of International Standardized Profiles - Part 1: Framework.*

ISO/IEC TR 10000-2: 1992*, Information technology - Framework and taxonomy of International Standardized Profiles - Part 2: Taxonomy.*

ISO/IEC 10021-1: 1990*, Information technology - Text Communication - Message-Oriented Text Interchange Systems (MOTIS) - Part 1: Service Overview. [see also CCITT Recommendation X.400(1988)]*

ISO/IEC 10021-2: 1990*, Information technology - Text Communication - Message-Oriented Text Interchange Systems (MOTIS) - Part 2: Overall Architecture. [see also CCITT Recommendation X.402(1988)]*

ISO/IEC 10021-4: 1990*, Information technology - Text Communication - Message-Oriented Text Interchange Systems (MOTIS) - Part 4: Message Transfer System: Abstract Service Definition and Procedures. [see also CCITT Recommendation X.411(1988)]*

ISO/IEC 10021-5: 1990*, Information technology - Text Communication - Message-Oriented Text Interchange Systems (MOTIS) - Part 5: Message Store: Abstract Service Definition. [see also CCITT Recommendation X.413(1988)]*

ISO/IEC 10021-6: 1990*, Information technology - Text Communication - Message-Oriented Text Interchange Systems (MOTIS) - Part 6: Protocol Specifications. [see also CCITT Recommendation X.419(1988)]*

ISO/IEC ISP 11188-1[1], *Information technology - International Standardized Profiles - Common upper layer requirements - Part 1: Basic connection oriented requirements.*

CCITT Recommendation X.248(1992), *Reliable Transfer Service Element - Protocol Implementation Conformance Statement (PICS) Proforma.*

CCITT Recommendation X.249(1992), *Remote Operations Service Element - Protocol Implementation Conformance Statement (PICS) Proforma.*

CCITT Recommendation X.400(1988), *Message handling system and service overview.*

CCITT Recommendation X.402(1988), *Message handling systems: Overall architecture.*

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.509(1988), *The Directory - Authentication framework.*

MHS Implementors' Guide, Version 8, March 1992 (CCITT Special Rapporteur's Group on Message Handling Systems and ISO/IEC JTC1/SC18/WG4 SWG on Messaging).

2. *Compliance with documentation requirements on conformance*

The Profiles documented in the submitted pDISP parts are in the class of Application Profiles using Connection-mode Transport Service. The documentation requirements in ISO/IEC TR 10000-1 on conformance (clauses 6.4-6.7, 8.4) have been met.

It had been intended that annex A of each of parts 3-5 of pDISP 10611 would be in the form of an IPRL based on the corresponding ISO/IEC 10021 PICS proforma. However, the development of MOTIS PICS proformas has now been suspended and it has therefore been necessary for pDISP 10611 to include complete ISPICS proformas for the MHS protocols (the alternative approach of a separate annex containing the assumed base standard PICS proforma was not considered appropriate in this case). These ISPICS proformas broadly follow the final drafts of CCITT Recommendations X.48x (April 1992), but the structure has been modified to some extent to take account of profiling requirements and the somewhat different conformance objectives. In addition, the identification of the base standard requirement has in some cases had to be interpreted or varied from that specified in the current CCITT PICS proforma, either due to the different classification scheme employed or where the base standard is unclear and it has been considered that the CCITT PICS proforma is in error.

3. *Non-compliance with base standards*

There are no aspects of actual or potential non-compliance with base standards.

4. *Amendments and technical corrigenda to base standards which may impact on interworking*

There are no approved amendments or technical corrigenda (errata) to base standards referenced in the profiles contained in the parts of this pDISP which in the view of the submitting organization may have a potential impact

[1] To be published.

on interworking.

C. Relationship To Other Publications

No national or regional standards are referenced in the parts of the submitted pDISP.

D. Profile Purpose

1. *Summary*

The AMH1n set of profiles is applicable to end systems operating in an Open Systems Interconnection (OSI) environment which form part of a distributed Message Handling Systems (MHS) environment as specified in ISO/IEC 10021 (MOTIS) and the equivalent CCITT X.400 Recommendations. The AMH1n profiles each specify a particular combination of OSI standards which collectively provide one of the MHS services as realised by an MHS protocol:

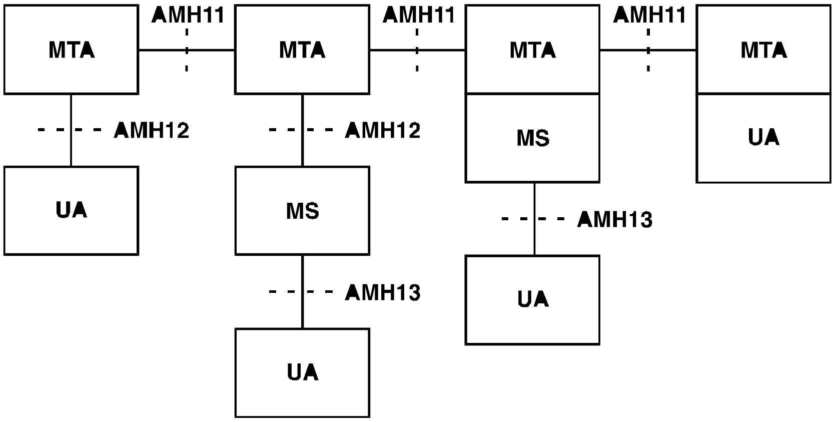
- AMH11 - Message Transfer (P1 protocol) - between message transfer agents (MTAs)
- AMH12 - Message Transfer System (MTS) Access (P3 protocol) - between a remote user agent (UA) and an MTA, and between a remote message store (MS) and an MTA
- AMH13 - Message Store (MS) Access (P7 protocol) - between a remote UA and an MS

Profile AMH11 is further subdivided into:

- AMH111 - requiring support of a ‘normal mode' OSI protocol infrastructure [as required by ISO/IEC 10021 (MOTIS)]
- AMH112 - requiring support of an ‘X.410 mode’ OSI protocol infrastructure [as required by the CCITT X.400(1988) Recommendations]

An MTA which conforms to profile AMH11 may conform to AMH111, or to AMH112, or to both.

Each AMH1n profile specifies the conformance requirements for all relevant MHS functional objects (ie, MTA, UA, MS). Two or more AMH1n profiles can be combined to establish the conformance requirements for the various physical configurations that may be achieved within the scope of the MHS base standards, as illustrated in the following diagram.



2. *Relationship to other ISPs*

The AMH1n set of profiles only covers Common Messaging - i.e., those aspects of the MHS base standards which are independent of a particular content type. Specific MHS applications are covered in separate content type-specific profile sets, of which the following are currently defined:

- AMH2n - Interpersonal Messaging
- AMH3n - EDI Messaging

Profiles in those sets which cover content type-specific use of MHS services do so by requiring conformance to the corresponding AMH1n profile plus support of any additional content type-specific requirements.

One or more of the AMH1n set of profiles may also be combined for the purposes of conformance without reference to any content type(s) that may be supported.

The AMH1n set of profiles is specified by reference to the common upper layer requirements (CULR): basic connection oriented requirements as specified in ISO/IEC ISP 11188-1.

E. pDISP Development Process

1. *Origin and development history*

Reasonably mature regional MHS profiles had been developed by both OIW and EWOS/ETSI prior to the development of the MHS ISPs. However, there were significant differences between these regional profiles, particularly with respect to their overall taxonomy and structure.

The parts of pDISP 10611 have been developed under the management of the MHS ISP Special Group (MISG). MISG was formed in early 1991 as a joint workshop initiative, comprising delegations from the MHS groups of the three regional workshops. It has provided a forum for developing and agreeing the MHS ISP taxonomy, resolving key issues and carrying out initial review of revised ISP drafts. All MISG decisions have been subject to ratification by the full meetings of the workshop MHS groups, which have also carried out detailed review of the ISP drafts.

MISG meetings to date are as follows:

1 May 29-31, 1991, Santa Monica, CA, USA

2 September 4-6, 1991, Brussels, Belgium

3 January 28-30, 1992, Tokyo, Japan

4 May 19-21, 1992, Vancouver, Canada

5 September 9-11, 1992, Oxford, UK

6 February 1-4, 1993, Kyoto, Japan

2. *Degree of openness and harmonization*

The working drafts of pDISP 10611 have been regularly reviewed by the MISG and separately by the MHS groups of all three regional workshops: AOW, EWOS/ETSI and OIW.

The parts of pDISP 10611 as submitted are fully harmonized between the three regional workshops and have been endorsed by the plenary assemblies of the three workshops (see appendix).

3. *Joint planning*

A revised taxonomy for MHS profiles was agreed between the three workshops and submitted to SGFS in April 1992. It was approved at the June 1992 meeting of SGFS and is included in the current published version of ISO/IEC TR 10000-2 : 1992.

Earlier drafts of the parts of pDISP 10611 were submitted to the SGFS Informal Quality Review service in August 1992, but no response has yet been received. The three regional workshops have since conducted their own final reviews and have approved the final texts for formal submission to SGFS subject to resolution of any outstanding issues to the satisfaction of the workshop delegations at the 6th MISG meeting in February 1993. This was achieved.

It is expected that all referenced base standards and ISPs will be ratified and published by the end of 1993.

F. ISP Content and Format

1. *Compliance with the requirements of TR 10000-1*

The requirements of clauses 6.3, 8 and annex A of ISO/IEC TR 10000-1 on the content and format of an ISP have been met.

2. *Divergence from the requirements of TR 10000-1*

There is no divergence from the requirements of ISO/IEC TR 10000-1 on the content and format of an ISP.

3. *Multi-part ISP structure*

The AMH1n set of profiles is specified as a multipart ISP consisting of the following parts:

Part 1: MHS service support.

> A common text part which provides functional description and specification of MHS service support and associated functionality as covered by the AMH1n set of profiles. It identifies what service support and functionality can be supported by each type of MHS component, divided into basic requirements (ie, required to be supported by all implementations) and zero or more optional functional groups (discrete sets of related functionality which are not required to be supported by all implementations). Such specifications are in many cases applicable to more than one MHS protocol or are otherwise concerned with component functionality which, although it can be verified via protocol, is not just related to protocol support. The specification in this part is therefore designed for reference by the following parts (which specify conformance requirements by protocol for each MHS component) and is additional to the protocol-specific requirements specified in those parts. Thus, although this part contains normative requirements, there is no separate conformance to this part (ie, it is not identified in the MHS taxonomy) since such requirements are only significant when referenced in the context of a particular protocol profile.

Part 2: Specification of ROSE, RTSE, ACSE, Presentation and Session protocols for use by MHS.

> A common text part which provides specification of the underlying protocol infrastructure requirements to support the various MHS application contexts. This is achieved as far as possible by reference to the Common Upper Layer Requirements (CULR): Basic connection oriented requirements ISP 11188-1, plus

specification of any further requirements which are either MHS-specific or otherwise not covered by part 1 of the CULR ISP (ROSE, RTSE).

Part 3: AMH11 - Message Transfer (P1).

This part covers message transfer between MTAs using the P1 Message Transfer Protocol. It specifies P1 support in terms of basic requirements and optional functional groups and defines conformance requirements for an MTA which supports transfer with respect to support of P1 and associated functionality (by reference to the common specifications in part 1).

Part 4: AMH12 - MTS Access (P3).

This part covers access to an MTS using the P3 MTS Access Protocol. It specifies P3 support in terms of basic requirements and optional functional groups and defines conformance requirements for an MTA which supports remote access, and for a remote MTS-user (ie, UA or MS), with respect to support of P3 and associated functionality (by reference to the common specifications in part 1).

Part 5: AMH13 - MS Access (P7).

This part covers access to an MS using the P7 MS Access Protocol. It specifies P7 support in terms of basic requirements and optional functional groups and defines the conformance requirements for an MS which supports remote access, and for a remote MS-user (ie, UA), with respect to support of P7 and associated functionality (by reference to the common specifications in part 1).

G. Any Other Information

None.

Appendices: Endorsement letters from the three regional workshops

TITLE: Information technology - International Standardized Profiles AMH1n -
Message Handling Systems - Common Messaging -
Part 1 : MHS Service Support

SOURCE: Project Editor (Jon Stranger, UK)

STATUS: DISP text, 1993-7-31

This document forms part of a proposed multipart ISP for MHS covering Common Messaging requirements (AMH1), as identified in the Taxonomy for International Standardized Profiles (ISO/IEC TR 10000-2 : 1992).

This revised DISP version reflects resolution of all remaining outstanding issues at the 6th MHS ISP Special Group (MISG) meeting (Kyoto, February 1-4, 1993) together with some editorial and minor errata which have been determined since submission to ISO/IEC JTC1/SGFS. The content of this document is considered by the MHS expert groups of the three regional workshops as harmonized.

The technical content of this document has been derived wherever possible from the existing EWOS/ETSI and OIW regional profiles in this area. However, differences between the content of this document and one or more regional profiles may exist.

Contents

Annexes

ISO/IEC Copyright Office _ Case Postale 56 _ CH-1211 Genève 20 _ Switzerland

Printed in Switzerland

Foreword

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

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC1. In addition to developing International Standards, ISO/IEC JTC1 has created a Special Group on Functional Standardization for the elaboration of International Standardized Profiles.

An International Standardized Profile is an internationally agreed, harmonized document which identifies a standard or group of standards, together with options and parameters, necessary to accomplish a function or set of functions.

Draft International Standardized Profiles are circulated to national bodies for voting. Publication as an International Standardized Profile requires approval by at least 75% of the national bodies casting a vote.

International Standardized Profile ISO/IEC ISP 10611-1 was prepared with the collaboration of:

- Asia-Oceania Workshop (AOW)

- European Workshop for Open Systems (EWOS) [jointly with the European Telecommunications Standards Institute (ETSI)]

- OSE Implementors' Workshop (OIW)

ISO/IEC ISP 10611 consists of the following parts, under the general title *Information technology - International Standardized Profiles AMH1n - Message Handling Systems - Common Messaging*:

- Part 1 : MHS Service Support

- Part 2 : Specification of ROSE, RTSE, ACSE, Presentation and Session Protocols for use by MHS

- Part 3 : AMH11 - Message Transfer (P1)

- Part 4 : AMH12 - MTS Access (P3)

- Part 5 : AMH13 - MS Access (P7)

This part of ISO/IEC ISP 10611 contains four annexes, of which annexes A and B are normative and annexes C and D are informative.

Introduction

This part of International Standardized Profile ISO/IEC ISP 10611 is defined within the context of Functional Standardization, in accordance with the principles specified by ISO/IEC TR 10000, “Framework and Taxonomy of International Standardized Profiles”. The context of Functional Standardization is one part of the overall field of Information Technology (IT) standardization activities, covering base standards, profiles, and registration mechanisms. A profile defines a combination of base standards that collectively perform a specific well-defined IT function. Profiles standardize the use of options and other variations in the base standards, and provide a basis for the development of uniform, internationally recognized system tests.

One of the most important rôles for an ISP is to serve as the basis for the development (by organizations other than ISO and IEC) of internationally recognized tests and test centres. ISPs are produced not simply to ‘legitimize' a particular choice of base standards and options, but to promote real system interoperability. The development and widespread acceptance of tests based on this and other ISPs is crucial to the successful realization of this goal.

The text for this part of ISO/IEC ISP 10611 was developed in close cooperation between the MHS Expert Groups of the three Regional Workshops: the North American OSE Implementors' Workshop (OIW), the European Workshop for Open Systems (EWOS) (jointly with the corresponding expert group of the European Telecommunications Standards Institute - ETSI) and the OSI Asia-Oceania Workshop (AOW). This part of ISO/IEC ISP 10611 is harmonized between these three Workshops and it has been ratified by the plenary assemblies of all three Workshops.

Information technology - International Standardized Profiles AMH1n - Message Handling Systems - Common Messaging

Part 1 : MHS Service Support

1 Scope

1.1 General

This part of ISO/IEC ISP 10611 contains the overall specifications of the support of MHS Elements of Service and associated MHS functionality which are generally not appropriate for consideration only from the perspective of a single MHS protocol. These specifications form part of the Common Messaging application functions, as defined in the parts of ISO/IEC ISP 10611, which form a common basis for content type-dependent International Standardized Profiles for MHS that will be developed. Such specifications are in many cases applicable to more than one MHS protocol or are otherwise concerned with component functionality which, although it can be verified via protocol, is not just related to protocol support. They are therefore designed to be referenced in the MHS Common Messaging application profiles ISO/IEC ISP 10611-3 (AMH11), ISO/IEC ISP 10611-4 (AMH12) and ISO/IEC ISP 10611-5 (AMH13), which specify the support of specific MHS protocols and associated functionality.

The specifications in this part of ISO/IEC ISP 10611 cover the provision and use of features associated with the Message Transfer (MT) Service (MTS) (as defined in clause 8 of ISO/IEC 10021-1), together with those features associated with intercommunication with Physical Delivery (PD) Services (as defined in clause 10 of ISO/IEC 10021-1). Features which are associated with the Message Store (MS) and User Agent (UA) which are content type-independent are also covered. Features which are specific to a particular content type (including the provision of services by a UA to an MHS user) are covered in separate content type-dependent ISPs.

The specifications in this part of ISO/IEC ISP 10611 are divided into **basic requirements**, which are required to be supported by all MHS implementations, and a number of optional **functional groups**, which cover significant discrete areas of related functionality which are not required to be supported by all implementations.

1.2 Position within the taxonomy

This part of ISO/IEC ISP 10611 is the first part, as common text, of a multipart ISP identified in ISO/IEC TR 10000-2 as “AMH1, Message Handling Systems - Common Messaging” (see also ISO/IEC TR 10000-1, 8.2 for the definition of multipart ISPs).

This part of ISO/IEC ISP 10611 does not, on its own, specify any profiles.

2 Normative references

The following documents contain provisions which, through reference in this text, constitute provisions of this part of ISO/IEC ISP 10611. At the time of publication, the editions indicated were valid. All documents are subject to revision, and parties to agreements based on this part of ISO/IEC ISP 10611 are warned against automatically applying any more recent editions of the documents listed below, since the nature of references made by ISPs to such documents is that they may be specific to a particular edition. Members of IEC and ISO maintain registers of currently valid International Standards and ISPs, and CCITT maintains published editions of its current Recommendations.

Amendments and corrigenda to the base standards referenced are listed in annex B.

NOTE - References in the body of this part of ISO/IEC ISP 10611 to specific clauses of ISO/IEC documents shall be considered to refer also to the corresponding clauses of the equivalent CCITT Recommendations (as noted below) unless otherwise stated.

ISO 7498-2: 1990, *Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture.*

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

ISO/IEC 9594-8: 1990, *Information technology - The Directory - Part 8: Authentication framework. [see also CCITT Recommendation X.509(1988)]*

ISO/IEC TR 10000-1: 1992*, Information technology - Framework and taxonomy of International Standardized Profiles - Part 1: Framework.*

ISO/IEC TR 10000-2: 1992*, Information technology - Framework and taxonomy of International Standardized Profiles - Part 2: Taxonomy.*

ISO/IEC 10021-1: 1990, *Information technology - Text Communication - Message-Oriented Text Interchange Systems (MOTIS) - Part 1: Service Overview. [see also CCITT Recommendation X.400(1988)]*

ISO/IEC 10021-2: 1990*, Information technology - Text Communication - Message-Oriented Text Interchange Systems (MOTIS) - Part 2: Overall Architecture. [see also CCITT Recommendation X.402(1988)]*

ISO/IEC 10021-4: 1990, *Information technology - Text Communication - Message-Oriented Text Interchange Systems (MOTIS) - Part 4: Message Transfer System: Abstract Service Definition and Procedures. [see also CCITT Recommendation X.411(1988)]*

ISO/IEC 10021-5: 1990, *Information technology - Text Communication - Message-Oriented Text Interchange Systems (MOTIS) - Part 5: Message Store: Abstract Service Definition. [see also CCITT Recommendation X.413(1988)]*

CCITT Recommendation X.400(1988)*, Message handling system and service overview.*

CCITT Recommendation X.402(1988)*, Message handling systems: Overall architecture.*

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.509(1988)*, The Directory - Authentication framework.*

MHS Implementors' Guide, Version 8, March 1992 (CCITT Special Rapporteur's Group on Message Handling Systems and ISO/IEC

JTC1/SC18/WG4 SWG on Messaging).

3 Definitions

For the purposes of this part of ISO/IEC ISP 10611, the following definitions apply.

Terms used in this part of ISO/IEC ISP 10611 are defined in the referenced base standards; in addition, the following terms are defined.

3.1 General

Basic requirement : an Element of Service, protocol element, procedural element or other identifiable feature specified in the base standards which is required to be supported by all MHS implementations.

Functional group : a specification of one or more related Elements of Service, protocol elements, procedural elements or other identifiable features specified in the base standards which together support a significant optional area of MHS functionality.

NOTE - A functional group can cover any combination of MHS features specified in the base standards for which the effect of implementation can be determined at a standardized external interface - i.e., via a standard OSI communications protocol (other forms of exposed interface, such as a standardized programmatic interface, are outside the scope of this version of ISO/IEC ISP 10611).

3.2 Support classification

To specify the support level of Elements of Service for this part of ISO/IEC ISP 10611, the following terminology is defined.

mandatory support (**m**) :

> **for origination**: a service provider shall be able to make the Element of Service available to a service user in the rôle of originator; a service user shall be able to use the Element of Service in the rôle of originator;
>
> **for processing**: a service provider shall implement all procedures specified in the base standards which are associated with the provision of the Element of Service (i.e., to be able to provide the full effect of the Element of Service);
>
> **for reception**: a service provider shall be able to make the Element of Service available to a service user in the rôle of recipient; a service user shall be able to use the Element of Service in the rôle of recipient.

optional support (**o**) : an implementation is not required to support the Element of Service. If support is claimed, then the Element of Service shall be treated as if it were specified as mandatory support.

conditional support (**c**) : the Element of Service shall be supported under the conditions specified in this part of ISO/IEC ISP 10611. If these conditions are met, the Element of Service shall be treated as if it were specified as mandatory support. If these conditions are not met, the Element of Service shall be treated as if it were specified as optional support (unless otherwise stated).

out of scope (**i**) : the Element of Service is outside the scope of this part of ISO/IEC ISP 10611 - i.e., it will not be the subject of an ISP conformance test. However, the handling of associated protocol elements may be specified separately in the subsequent parts of this ISP.

not applicable (**–**) : the Element of Service is not applicable in the particular context in which this classification is used.

4 Abbreviations

84IW	84 Interworking
AMH	Application Message Handling
ASN.1	Abstract Syntax Notation One
COMPUSEC	Computer security
COMSEC	Communications security
CV	Conversion
DIR	Use of Directory
DL	Distribution List
DSA	Directory system agent
DUA	Directory user agent
EoS	Element of Service
FG	Functional group
ISP	International Standardized Profile
LD	Latest Delivery
MHS	Message Handling Systems
MLS	Multi-Level Security
MS	Message store
MT	Message transfer
MTA	Message transfer agent
MTS	Message Transfer System
OSI	Open Systems Interconnection
PD	Physical Delivery
PDAU	Physical delivery access unit
RED	Redirection
RoC	Return of Contents
SEC	Security
UA	User agent

Support level for Elements of Service (see 3.2):

m	mandatory support
o	optional support
c	conditional support
i	out of scope
–	not applicable

5 Conformance

No conformance requirements are specified in this part of ISO/IEC ISP 10611.

NOTE - This part of ISO/IEC ISP 10611 is a reference specification of the basic requirements and functional groups covered by the AMH1n set of profiles and is additional to the protocol-specific requirements specified in the following parts of ISO/IEC ISP 10611.

Although this part of ISO/IEC ISP 10611 contains normative requirements, there is no separate conformance to this part (i.e., it is not identified in the MHS taxonomy in ISO/IEC TR 10000-2) since such requirements are only significant when referenced in the context of a particular protocol.

Conformance requirements are specified by protocol for each MHS component in the following parts of ISO/IEC ISP 10611 with reference to the specifications in this part. Support of functionality as specified in this part may only be verifiable where the effect of implementation can be determined at a standardized external interface - i.e., via a standard OSI communications protocol. Further, the provision of Elements of Service and other functionality at a service interface will not necessarily be verifiable unless such interface is realized in the form of a standard OSI communications protocol. Other forms of exposed interface (such as a human user interface or a standardized programmatic interface) may be provided, but are not required for conformance to this version of ISO/IEC ISP 10611.

6 Basic requirements

Annex A specifies the basic requirements for support of MHS Elements of Service (EoS) for conformance to ISO/IEC ISP 10611. Basic requirements specify the level of support required by all MHS implementations, as appropriate to each type of MHS component - i.e., MTA, MS or UA (as MTS-user or MS-user, as relevant).

NOTE - ISO/IEC ISP 10611 is confined to the provision of services by MTAs and MSs, and the use of such services by MTS-users and MS-users. It does not cover the provision of such services by UAs to MHS users, which is specified in content type-specific profiles.

It shall be stated in the PICS which content type and encoded information type values are supported.

7 Functional groups

Annex A also specifies any additional requirements for support of MHS EoS if support of an optional functional group (FG) is claimed, as appropriate to each type of MHS component. The following clauses summarize the functionality supported by each of the optional FGs and identify any particular requirements or implementation considerations which are outside the scope of formal conformance to ISO/IEC ISP 10611. A summary of the functional groups, identifying which may be supported (Y) and which are not applicable (N) for each type of MHS component (i.e., MTA, MS or UA - whether as MTS-user or as MS-user is not distinguished), is given in the following table.

Table 1 - Summary of AMH1n optional functional groups

Functional Group	MTA	MS	UA
Conversion (CV)	Y	N	N[1]
Distribution List (DL)	Y	N	N
Physical Delivery (PD)	Y	N	Y
Redirection (RED)	Y	N	N[1]
Latest Delivery (LD)	Y	N	Y
Return of Contents (RoC)	Y	N	Y
Security (SEC)	Y	Y	Y
Use of Directory (DIR)	Y	N	Y
84 Interworking (84IW)	Y	N	N[1]

[1] UA functionality may be further defined in content type-dependent profiles.

7.1 Conversion (CV)

The Conversion FG covers support of those EoS which provide the functionality required to perform the action of encoded information type conversion. Support of the CV FG is only applicable to an MTA.

NOTE - Support of EoS associated with conversion prohibition is a basic requirement, but this does not imply a capability to perform conversion.

Either or both of Explicit Conversion and Implicit Conversion shall be supported. A conforming implementation shall obey the rules specified in clauses 14.3.5 and 14.3.9 of ISO/IEC 10021-4.

Conformance to ISO/IEC ISP 10611 does not require the capability to perform any specific conversions. Further specific requirements may be included in content type-dependent International Standardized Profiles for MHS that will be developed or may otherwise be separately specified. It shall be stated in the PICS which encoded information type conversions the implementation can perform, for the type(s) of conversion (i.e., explicit or implicit) for which support is claimed. The PICS shall also state the conditions under which loss of information is determined (if at all) for each encoded information type conversion for which support is claimed.

NOTE - It may not be possible to verify support of conversion in the absence of additional specification which is related to one or more identified content types.

7.2 Distribution List (DL)

The Distribution List FG covers all issues relating to the performance of distribution list (DL) expansion. Support of the DL FG is only applicable to an MTA.

NOTE - Other aspects concerned with the use of DLs (e.g., the ability to submit a message specifying a recipient which is a DL) are basic requirements. Similarly, it is a basic requirement that an MTA must be able to receive and handle correctly a message that reflects prior DL expansion.

Conformance to ISO/IEC ISP 10611 does not require any DL management capability other than as specified in clause 14.3.10 of ISO/IEC 10021-4. Any further specification will be implementation-dependent.

7.3 Physical Delivery (PD)

The Physical Delivery FG is concerned with access to physical delivery (i.e., postal, courier, etc.) services. The PD FG comprises two separate and distinct parts:

- support of PD EoS on submission;
- support of a co-located physical delivery access unit (PDAU).

Support of PD EoS on submission is applicable to an MTA or a UA. Support of a PDAU is only applicable to an MTA. If an MTA supports a PDAU and also supports message submission, then it shall also support PD EoS on submission.

Support of the PD FG also requires support of corresponding O/R address extension attributes.

If the PDAU generates any error on export, then the MTA shall generate a non-delivery report or take other appropriate action (e.g., alternate recipient processing). All other processing concerned with the actual physical rendition and delivery of the message is outside the scope of ISO/IEC ISP 10611.

7.4 Redirection (RED)

The Redirection FG covers support of those EoS which provide the functionality required to perform the actions associated with the delivery of a message to a recipient other than the one initially specified by the originator. Support of the RED FG is only applicable to an MTA.

NOTE - Support of EoS associated with the prevention of redirection is a basic requirement, but this does not imply a capability to perform redirection. Similarly, support of the Alternate Recipient Allowed EoS is a basic requirement, but this does not imply a capability to perform alternate recipient assignment.

A conforming implementation shall obey the rules specified in clause 14.3 of ISO/IEC 10021-4.

The means by which the Alternate Recipient Assignment EoS is achieved is outside the scope of ISO/IEC ISP 10611.

7.5 Latest Delivery (LD)

The Latest Delivery FG covers support of the Latest Delivery EoS - i.e., the functionality required to cause non-delivery to occur if a latest delivery time specified by the originator has expired. Support of the LD FG is applicable to an MTA or a UA. If an MTA supports the LD FG and also supports message submission, then it shall also support the Latest Delivery EoS on submission.

NOTE - Latest delivery designation is assured only if it is supported by at least the delivering MTA.

7.6 Return of Contents (RoC)

The Return of Contents FG covers support of the Return of Contents EoS - i.e., the functionality required to cause the contents of a submitted message to be returned in any non-delivery notification if so requested by the originator. Support of the RoC FG is applicable to an MTA or a UA. If an MTA supports the RoC FG and also supports message submission, then it shall also support the Return of Contents EoS on submission.

NOTE - Return of contents is assured only if it is supported by all MTAs through which the message might pass.

7.7 Security (SEC)

7.7.1 Overview

The Security FG covers the provision of secure messaging and is specified as three **security classes** which are incremental subsets of the security features available in the MHS base standards:

S0 This security class only requires security functions which are applicable between MTS-users. Consequently security mechanisms are implemented within the MTS-user. An MTA is only required to support the syntax of the security services on submission and delivery (support of the syntax on relaying is a basic requirement). An MTA is not expected to understand the semantics of the security services.

S1 This security class requires security functionality within both the MTS-user and the MTS. The MTS security functionality is only required to achieve secure access management. As with S0, most of the security mechanisms are implemented within an MTS user. S1 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 adds security functions within MTAs and the MTS. The main security function added within this class is authentication within the MTS, and hence non-repudiation can also be provided.

In addition, each of the three security classes has a variant (denoted as **S0C**, **S1C** and **S2C**) which requires support of end-to-end content confidentiality.

Double enveloping can be used with each security class as an optional extension, but is outside the scope of conformance to ISO/IEC ISP 10611 and will be subject to bilateral agreement.

Support of the SEC FG is applicable to an MTA, an MS or a UA (either as MTS-user or as MS-user) and requires as a minimum support of security class S0.

Unless otherwise stated, 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, but this is outside the scope of an ISP.

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

The following table summarizes the requirements of the security classes on an MTS-user and on an MTA.

Table 2 - Overview of the SEC security classes

Security Class	MTS-user	MTA
Basic		Supports relay of security EoS
S0	Content integrity Proof of delivery Origin authentication (end-to-end)	Supports submission and delivery of security EoS
S1	As S0 plus: Message security labelling Security context Security management	As S0 plus: Peer entity authentication Message security labelling Security context Security management
S2	As S1 plus: Origin authentication checks Proof of submission	As S1 plus: Origin authentication checks Proof of submission
SnC	As Sn plus: Content confidentiality	As Sn

The incremental functionality of the security classes can be represented diagrammatically as shown in figure 1.

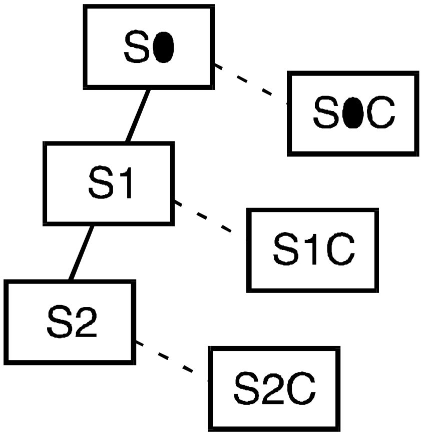


Figure 1 - Incremental functionality of the SEC security classes

7.7.2 Secure interworking

Interworking between implementations supporting different security classes can be achieved in terms of any common class(es) supported. As specified in the base standards, an implementation which supports secure access management shall check the label of a message, probe or report against the security context. There is no negotiation of security class during association establishment.

The security class in force is identified using the security-policy-identifier within a security label, as specified in table 3. Such generic security-policy-identifiers only imply support of the MHS security services as specified for these security classes in this part of ISO/IEC ISP 10611. No other COMSEC or COMPUSEC functionality can be assumed by use of such security-policy-identifiers. More specific security policies may be based on one or more of the security classes as defined in this clause but will require use of registered security-policy-identifiers for private secure interworking.

A security label may additionally contain one or more of security-classification, security-categories and privacy-mark. Table 3 specifies a minimum set of values for security-categories. Again, further values may be registered for private secure interworking. However, in all cases, the precise semantics of security-categories are outside the scope of this ISP and will require bilateral agreement.

Table 3 - Security label identifiers

Identifier	Value
id-mhs-security	{ iso(1) identified-organization(3) ewos(16) eg(2) mhs(4) security(4) }
id-policy-identifier	{ id-mhs-security 1 }
security-policy-identifiers:	
security-class-S0	{ id-policy-identifier 0 0 }
security class S0C	{ id-policy-identifier 0 1 }
security-class-S1	{ id-policy-identifier 1 0 }
security-class-S1C	{ id-policy-identifier 1 1 }
security-class-S2	{ id-policy-identifier 2 0 }
security-class-S2C	{ id-policy-identifier 2 1 }
id-category-identifier	{ id-mhs-security 2 }
security-categories:	
private	{ id-category-identifier 0 }
confidence	{ id-category-identifier 1 }
commercial-in-confidence	{ id-category-identifier 2 }
management-in-confidence	{ id-category-identifier 3 }
personal-in-confidence	{ id-category-identifier 4 }

The Security Context security service ensures that a message security label matches at least one of the set of labels specified in the security context established between the communicating entities. An implementation which supports this service shall as a minimum support exact 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 will need to be elaborated in the security context (see also annex C).

7.7.3 Description of the security classes

The following tables identify the security services covered by each of the security classes within the SEC FG. Where the classification of a security service does not change for the higher security classes, then the security service is not repeated in the tables for those higher security classes. Figure 2 explains the column headings used in the tables, which identify which MHS system components are involved in the provision and use of each security service.

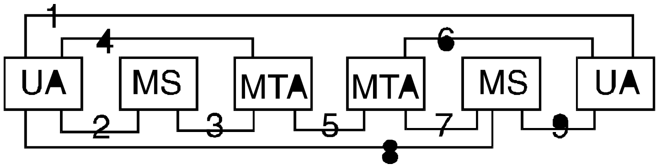


Figure 2 - Key to security class tables

7.7.3.1 Security class S0

Table 4 - Security class S0

Security Service	1	2	3	4	5	6	7	8	9
	UA/ UA	UA/ MS	MS/ MTA	UA/ MTA	MTA/ MTA	MTA/ UA	MTA/ MS	MS/ UA	MS/ UA
ORIGIN AUTHENTICATION									
Message Origin Authentication[1]	m	i	–	i	–	–	–	–	–
Probe Origin Authentication	–	i	–	i	–	–	–	–	–
Report Origin Authentication	–	–	–	–	i	i	i	–	–
Proof of Submission	–	–	–	–	–	i	–	–	–
Proof of Delivery	m	–	–	–	–	–	–	m[8]	–
SECURE ACCESS MANAGEMENT									
Peer Entity Authentication[2,6]	–	o	o	o	o	o	o	–	o
Security Context	–	o	o	o	o	o	o	–	o
DATA CONFIDENTIALITY									
Connection Confidentiality	–	i	i	i	i	i	i	–	i
Content Confidentiality	o	–	–	–	–	–	–	–	–
Message Flow Confidentiality	i	–	–	–	–	–	–	–	–
DATA INTEGRITY									
Connection Integrity	–	i	i	i	i	i	i	–	i
Content Integrity	m	–	–	–	–	–	–	–	–
Message Sequence Integrity[4]	o	–	–	–	–	–	–	–	–
NON-REPUDIATION									
Non-repudiation of Origin[1,5]	o	–	–	i	–	–	–	–	–
Non-repudiation of Submission	–	–	–	–	–	i	–	–	–
Non-repudiation of Delivery[5]	o	–	–	–	–	–	–	o[8]	–
Message Security Labelling[2,3]	o	o	o	o	o	o	o	o	o
SECURITY MANAGEMENT									
Change Credentials	–	o	–	o	i[7]	o	o	–	–
Register	–	o	–	o	i[7]	–	–	–	–
MS-Register	–	o	–	–	–	–	–	–	–

NOTES

1 Only provided to the message recipient (using the Message Argument Integrity security element).

2 Using either asymmetric or symmetric algorithms as identified by the algorithm identifier.

3 When security labelling is used, the security-policy-identifier shall be included.

4 Allocation and management of sequence numbers is outside the scope of this ISP and is subject to bilateral agreement.

5 Using either a trusted notary (symmetric) or using certificates and tokens which are not repudiable (asymmetric).

6 Authentication between co-located objects is a local issue.

7 These services are expected to be provided by non-standard management services and are therefore outside the scope of this ISP.

8 Non-repudiation of Delivery can only be provided when the Proof of Delivery service is used. However, 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.

7.7.3.2 Security class S1

Table 5 - Security class S1

Security Service	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
As S0 plus:	**UA/ UA**	**UA/ MS**	**MS/ MTA**	**UA/ MTA**	**MTA/ MTA**	**MTA/ UA**	**MTA/ MS**	**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 CONFIDENTIALITY									
Connection Confidentiality[6]	–	i	i	i	i	i	i	–	i
DATA INTEGRITY									
Connection Integrity[6]	–	i	i	i	i	i	i	–	i
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									
Change Credentials	–	m	–	m	i[5]	m	m	–	–
Register	–	m	–	m	i[5]	–	–	–	–
MS-Register	–	m	–	–	–	–	–	–	–

NOTES

1 Shall always be used.

2 Only provided to the message recipient (using the Message Argument Integrity security element.

3 Using either asymmetric or symmetric algorithms as identified by the algorithm identifier.

4 Authentication between co-located 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 ISP.

6 Shall be provided as defined in clause 10 of ISO/IEC 10021-2 and in ISO 7498-2.

7.7.3.3 Security class S2

Table 6 - Security class S2

Security Service	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
As S1 plus:	**UA/ UA**	**UA/ MS**	**MS/ MTA**	**UA/ MTA**	**MTA/ MTA**	**MTA/ UA**	**MTA/ MS**	**MS/ UA**	**MS/ UA**
ORIGIN AUTHENTICATION									
Message Origin Authentication[3]	m[1]	m[1]	–	m[1]	–	–	–	–	–
Probe Origin Authentication	–	m[1]	–	m[1]	–	–	–	–	–
Report Origin Authentication	–	–	–	–	m[1]	m[1]	m[1]	–	–
Proof of Submission	–	–	–	–	–	m	–	–	–
NON-REPUDIATION									
Non-repudiation of Origin[1,5]	m[4]	–	–	m[2]	–	–	–	–	–
Non-repudiation of Submission	–	–	–	–	–	m[2]	–	–	–
Non-repudiation of Delivery[5]	m[4]	–	–	–	–	–	–	m[2]	–

NOTES

1 Shall always be used.

2 Using an asymmetric mechanism (i.e., certificates and tokens which are non-repudiable) for authentication within MTAs and the MTS.

3 Using the Message Origin Authentication Check security element.

4 Using either a trusted notary (symmetric) or non-repudiable certificates and tokens (asymmetric).

7.7.3.4 Confidential security class variants SnC

Table 7 - Confidential security class variants SnC

Security Service	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
As Sn plus:	**UA/ UA**	**UA/ MS**	**MS/ MTA**	**UA/ MTA**	**MTA/ MTA**	**MTA/ UA**	**MTA/ MS**	**MS/ UA**	**MS/ UA**
DATA CONFIDENTIALITY									
Content Confidentiality	m	–	–	–	–	–	–	–	–

7.8 Use of Directory (DIR)

The Use of Directory FG covers support of the Designation of Recipient by Directory Name EoS as follows:

- support of specification of a recipient by means of a directory name by an MTS-user or an MTA on submission;

- support of access to a directory service by an MTA to obtain one or more O/R addresses (either on submission or subsequently if an O/R address is absent or determined to be invalid and a directory name is present).

NOTE - A directory may also be used directly by MHS users to obtain information to assist in the submission of messages. However, such use is not necessarily MHS-specific and is therefore outside the scope of this ISP.

For a UA, support of the DIR FG only requires the ability to submit a message with one or more O/R names specified using a directory name, as specified in clause 8.5.5 of ISO/IEC 10021-4. Whether or not the UA also has the capability to access a directory directly is outside the scope of ISO/IEC ISP 10611.

An MTA may access a directory service using a Directory User Agent (DUA). The interface between the MTA and the DUA is a local matter and is outside the scope of ISO/IEC ISP 10611. Similarly, the interaction between the DUA and one or more Directory System Agents (DSAs) comprising the directory service is also outside the scope of ISO/IEC ISP 10611. The only information that is assumed to be capable of being returned by the directory service in this version of ISO/IEC ISP 10611 is an attribute containing one or more O/R addresses.

NOTE - The MTS may also use a directory service to obtain information, for example, that may be used in the routing of messages. However, such applications of a directory service are not defined by the MHS base standards and are therefore outside the scope of ISO/IEC ISP 10611.

7.9 84 Interworking (84IW)

The 84 Interworking functional group covers interworking between implementations conforming to ISO/IEC ISP 10611 (hereafter referred to as ‘1988 systems') and implementations conforming to the CCITT X.400(1984) Recommendations (hereafter referred to as ‘1984 systems'). Support of the 84IW FG is only applicable to an MTA and is not applicable unless the MTA supports the P1 mts-transfer-protocol-1984 application context (see ISO/IEC ISP 10611-3).

Support of the 84IW FG requires observance of the interworking rules defined in annex B of ISO/IEC 10021-6. Additional recommended practices for interworking with 1984 systems are described in annex D.

8 Naming and addressing

8.1 O/R address attribute encodings

The basic rules governing different encodings (where permitted) of O/R address attributes are specified in clause 18.2 of ISO/IEC 10021-2.

An MTA shall be able to accept on submission, to transfer and to deliver (according to which ports are supported) messages containing O/R address attributes with any valid encoding. No character repertoire restrictions apply - i.e., all repertoires specified for Teletex String in ISO 8824 shall be supported.

A UA shall be able to submit and to accept on delivery messages containing O/R address attributes with any valid encoding within the mnemonic form. However, support of particular character repertoires and the methods by which such values are captured on origination and made available to the MHS user on reception are outside the scope of this ISP.

8.2 O/R address attribute equivalence

The following equivalence rules apply when comparing a provided O/R address with a collection of known O/R addresses to determine delivery, and are in addition to those specified in clause 18.4 of ISO/IEC 10021-2:

- If the provided O/R address can be determined to be an unambiguous underspecification of a known O/R address, the O/R addresses are equivalent.

  NOTE 1 - Underspecification means that some attributes (or components of structured attributes) are present in the known O/R address but are not present in the provided O/R address. Underspecification does not mean partial value (e.g., substring) equivalence when the same attributes are present in both O/R addresses.

- Overspecified O/R addresses are not equivalent.

  NOTE 2 - Overspecification means that more attributes (or components of structured attributes) are present in the provided O/R address than are present in the known O/R address. However, unrecognized domain-defined attributes may be ignored when determining overspecification, subject to the local policy of the recipient domain.

- Attributes that are present in both Teletex String and Printable String encodings in the same O/R address may be considered equivalent by virtue of their registration for the same UA. MTAs are not responsible for verifying the equivalence of different encodings of the same attribute. Either encoding of an attribute may be used for the purposes of routing and delivery.

Further specification of repertoire-specific matching rules is outside the scope of ISO/IEC ISP 10611.

8.3 Routing capability

The capability of an MTA to determine the route to another MTA or destination MTS-user is described in clause 19 of ISO/IEC 10021-2. ISO/IEC ISP 10611 does not specify any requirements with respect to which O/R address attributes must be capable of being used for route determination purposes. For any MTA which support message transfer, it shall be stated in the PICS which O/R address attributes may be used for onward route determination and any constraints (e.g., whether routing can be based on specific values of the attribute or only on the presence of the attribute, any limitations on the range of values, character repertoires, etc.) which may apply.

8.4 Validation of O/R addresses

As specified in clause 14.6.1.4 of ISO/IEC 10021-4, an MTA shall verify on submission that O/R addresses comply with the forms defined in ISO/IEC 10021-2.

9 Error and exception handling

The upper bounds defined in annex B of ISO/IEC 10021-4 and in annex E of ISO/IEC 10021-5 are normative for the purposes of this ISP.

An implementation shall not generate elements which exceed such bounds.

An implementation detecting a violation of such bounds may generate a size-constraint-violation, but is not required to do so.

An implementation is not required to be able to accept elements up to such bounds where an appropriate error indication (e.g., content-too-long, too-many-recipients) is defined in the base standards.

Annex A

(normative)

Elements of Service

In the event of a discrepancy becoming apparent in the body of this part of ISO/IEC ISP 10611 and the tables in this annex, this annex is to take precedence.

A.1 MT Elements of Service

In the following tables, the "Basic" column reflects the basic requirements for conformance to ISO/IEC ISP 10611 - i.e., the minimum level of support required by all MHS implementations (see clause 6). The "Functional Group" column specifies any additional support requirements if support of an optional functional group is claimed (see clause 7). Each column is then further subdivided into support for origination ("Orig"), processing ("Proc") and reception ("Rec") as defined in 3.2, together with the abbreviated name of the functional group ("FG") in the case of the second column. The origination and reception columns are further subdivided to distinguish the support required for an MTA from that for an MTS-user (the latter refers only to the use of MT services, not whether such services are made available to the MHS user, and may be further qualified in a content type-dependent profile).

Table A.1 - Elements of Service Belonging to The Basic MT Service

Element of Service	Basic					Functional Group					
	Orig.		Proc.	Rec.		FG	Orig.		Proc.	Rec.	
	MTS-user	MTA		MTA	MTS-user		MTS-user	MTA		MTA	MTS-user
Access Management[1]	m	m	m	m	m						
Content Type Indication	m	m	m	m	m						
Converted Indication	–	–	m	m	m						
Delivery Time Stamp Indication	–	–	m	m	m						
Message Identification	m	m	m	m	m						
Non-delivery Notification	m	m	m	–	–						
Original Encoded Information Types Indication	m	m	m	m	m						
Submission Time Stamp Indication	m	m	m	m	m						
User/UA Capabilities Registration[1]	–	–	m	m	m						

NOTES

[1] Implementation of this EoS is a local matter and will need to be performed using trusted functionality when implemented in combination with the SEC FG.

Table A.2 - MT Service Optional User Facilities

Element of Service	Basic					Functional Group					
	Orig.		Proc.	Rec.		FG	Orig.		Proc.	Rec.	
	MTS-user	MTA		MTA	MTS-user		MTS-user	MTA		MTA	MTS-user
Alternate Recipient Allowed	o	m	c[2]	c[2]	–	RED			m	m	
Alternate Recipient Assignment[3]	–	–	o	–	–	RED			m		
Content Confidentiality	o	o	–	o	o	SEC[1]					
Content Integrity	o	o	–	o	o	SEC[1]					
Conversion Prohibition	m	m	c[4]	m	m	CV			m		
Conversion Prohibition in Case of Loss of Information	o	m	c[5]	m	o	CV			m		
Deferred Delivery	o	m	m	–	–						
Deferred Delivery Cancellation[6]	o	m	m	–	–						
Delivery Notification	m	m	m	–	–						
Designation of Recipient by Directory Name	o	o	o	–	–	DIR	m	m	m		
Disclosure of Other Recipients	o	m	m	m	m						
DL Expansion History Indication	–	–	c[7]	m	o	DL			m		
DL Expansion Prohibited	m[8]	m	c[7]	–	–	DL			m		
Explicit Conversion	o	m	o	–	–	CV			c[10]		
Grade of Delivery Selection	m	m	m	m	m						
Hold for Delivery	–	–	c[9]	c[9]	o						
Implicit Conversion	–	–	o	–	–	CV			c[10]		
Latest Delivery Designation	o	o	o	–	–	LD	m	m	m		
Message Flow Confidentiality	i	i	i	i	i						
Message Origin Authentication	o	o	i	o	o	SEC[1]					
Message Security Labelling	o	o	o	o	o	SEC[1]					
Message Sequence Integrity	o	o	–	o	o	SEC[1]					
Multi-destination Delivery	m	m	m	–	–						
Non-repudiation of Delivery	o	o	o	o	o	SEC[1]					

Non-repudiation of Origin	o	o	o	o	o	SEC[1]					
Non-repudiation of Submission	i	i	i	–	–	SEC[1]					
Originator Requested Alternate Recipient	o	o	o	–	–	RED		m	m		
Prevention of Non-delivery Notification	o	m	m	–	–						
Probe[11]	o	m	m	–	–						
Probe Origin Authentication	i	i	i	–	–	SEC[1]					
Proof of Delivery	o	o	–	o	o	SEC[1]					
Proof of Submission	i	i	i	–	–	SEC[1]					
Redirection Disallowed by Originator	m[8]	m	c[12]	–	–						
Redirection of Incoming Messages	–	–	o	o	o	RED			m	m	
Report Origin Authentication	i	i	i	i	i	SEC[1]					
Requested Preferred Delivery Method	o	o	o	o	–						
Restricted Delivery	–	–	i	i	i						
Return of Content	o	o	o	–	–	RoC	m	m	m		
Secure Access Management	o	o	o	o	o	SEC[1]					
Use of Distribution List	m[13]	m[13]	o	–	–	DL			m		

NOTES

1 See table A.5

2 Support of this EoS is mandatory if Alternate Recipient Assignment is supported

3 The method by which an alternate recipient is specified to the MTA is outside the scope of this ISP

4 Support of this EoS is mandatory if Implicit Conversion is supported

5 Support of this EoS is mandatory if any form of conversion is supported. However, as loss of information is not fully defined in the base standards, it will in some circumstances be a local matter to determine if loss of information would occur. If the implementation cannot determine whether loss of information would occur, then it shall treat such a request in a similar manner as Conversion Prohibition

6 Messages should be held in the originating MTA to provide support for this EoS

7 Support of this EoS is mandatory if DL expansion is supported

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

9 Support of this EoS is mandatory when using the P3 protocol. Implementation is a local matter in the case of a co-located MTS-user

10 The CV FG requires support of at least one of Explicit Conversion and Implicit Conversion

11 Although support of this EoS by MTAs is required for conformance to the base standards, it is recommended that support by MTS-users is not required

12 Support of this EoS is mandatory if Redirection of Incoming Messages is supported

13 Use of Distribution List on submission is always possible as DLs cannot be distinguished from other O/R addresses

Table A.3 - Elements of Service Belonging to the Base MH/PD Service Intercommunication

Element of Service	**Basic**					**Functional Group**					
	Orig.		**Proc.**	**Rec.**		**FG**	**Orig.**		**Proc.**	**Rec.**	
	MTS-user	**MTA**		**MTA**	**PDAU**		**MTS-user**	**MTA**		**MTA**	**PDAU**
Basic Physical Rendition	o	o	–	o	o	PD	m	m		m	m
Ordinary Mail	o	o	–	o	o	PD	m	m		m	m
Physical Forwarding Allowed	o	o	–	o	o	PD	m	m		m	m
Undeliverable Mail with Return of Physical Message	o	o	–	o	o	PD	m	m		m	m

Table A.4 - Optional User Facilities for MH/PD Service Intercommunication

Element of Service	Basic					Functional Group					
	Orig.		Proc.	Rec.		FG	Orig.		Proc.	Rec.	
	MTS-user	MTA		MTA	PDAU		MTS-user	MTA		MTA	PDAU
Additional Physical Rendition	o	o	–	o	o	PD		m			
Counter Collection	o	o	–	o	o	PD	m	m		m	m
Counter Collection with Advice	o	o	–	o	o	PD		m			
Delivery via Bureaufax Service	o	o	–	o	o	PD		m			
EMS (Express Mail Service)	o	o	–	o	o	PD	c[1]	m		c[1]	c[2]
Physical Delivery Notification by MHS	o	o	–	o	o	PD		m			
Physical Delivery Notification by PDS	o	o	–	o	o	PD		m			
Physical Forwarding Prohibited	o	o	–	o	o	PD	m	m		m	m
Registered Mail	o	o	–	o	o	PD		m			
Registered Mail to Addressee in Person	o	o	–	o	o	PD		m			
Request for Forwarding Address	o	o	–	o	o	PD		m			
Special Delivery	o	o	–	o	o	PD	c[1]	m		c[1]	c[2]

NOTES

1 At least one of these EoS must be supported

2 This EoS must be supported by the PDAU if it is supported by the MTA

Table A.5 - Security Services

Element of Service	**Security Class**					
	S0		**S1**		**S2**	
	MTS-user	**MTA**	**MTS-user**	**MTA**	**MTS-user**	**MTA**
Content Confidentiality[3]	c[1]	m	c[1]	m	c[1]	m
Content Integrity[3]	m	m	m[2]	m[2]	m[2]	m[2]
Message Origin Authentication	m[4]	m[3]	m[2,4]	m[2,3]	m[2]	m[2]
Message Security Labelling	o	m[3]	m[2]	m[2]	m[2]	m[2]
Message Sequence Integrity[3]	o	m	o	m	o	m
Non-repudiation of Delivery	o	m[3]	o	m[3]	m	m
Non-repudiation of Origin	o	m[3]	o	m[3]	m	m
Non-repudiation of Submission	i	i	i	i	m	m
Probe Origin Authentication	i	i	i	i	m[2]	m[2]
Proof of Delivery	m	m	m	m	m	m
Proof of Submission	i	i	i	i	m	m
Report Origin Authentication	i	i	i	i	m	m
Secure Access Management	o	o	m[2]	m[2]	m[2]	m[2]

NOTES

1 Support becomes m if support of an SnC confidential class variant is claimed

2 This EoS shall always be used and an MTA shall verify that the associated element(s) is(are) always present

3 An MTA is not expected to take any action other than to support the syntax of the element(s) concerned (except where note 2 applies)

4 MTS-user to MTS-user only

A.2 MS Elements of Service

In the following tables, the "Basic" column reflects the basic requirements for conformance to ISO/IEC ISP 10611 - i.e., the minimum level of support required by all MHS implementations (see clause 6). The "Functional Group" column specifies any additional support requirements if support of an optional functional group is claimed (see clause 7), together with the abbreviated name of the functional group ("FG"). Each column is further subdivided to distinguish the support required for an MS from that for an MS-user - i.e., UA (the latter refers only to the use of MS services, not whether such services are made available to the MHS user, and may be further qualified in a content type-dependent profile).

Table A.6 - Base Message Store

Element of Service	Basic		Functional Group		
	UA	MS	FG	UA	MS
MS Register	o	m			
Stored Message Deletion	m	m			
Stored Message Fetching	m	m			
Stored Message Listing	o	m			
Stored Message Summary	o	m			

Table A.7 - MS Optional User Facilities

Element of Service	Basic		Functional Group		
	UA	MS	FG	UA	MS
Stored Message Alert	o	o			
Stored Message Auto-forward	o	o			

Annex B

(normative)

Amendments and corrigenda

International Standards are subject to constant review and revision by the ISO/IEC Technical Committees concerned. The following amendments and corrigenda are approved by ISO/IEC JTC1 and are considered as normative references in this part of ISO/IEC ISP 10611.

NOTE - Corresponding corrigenda to the equivalent CCITT Recommendations are contained in the joint CCITT/ISO MHS Implementor's Guide (version 8).

MOTIS

ISO/IEC 10021-1/Cor.1:1991

ISO/IEC 10021-1/Cor.2:1991

ISO/IEC 10021-1/Cor.3:1992

ISO/IEC 10021-1/Cor.4:1992

ISO/IEC 10021-1/Cor.5:1992

ISO/IEC 10021-2/Cor.1:1991

ISO/IEC 10021-2/Cor.2:1991

ISO/IEC 10021-2/Cor.3:1992

ISO/IEC 10021-2/Cor.4:1992

ISO/IEC 10021-4/Cor.1:1991

ISO/IEC 10021-4/Cor.2:1991

ISO/IEC 10021-4/Cor.3:1992

ISO/IEC 10021-4/Cor.4:1992

ISO/IEC 10021-4/Cor.5:1992

ISO/IEC 10021-5/Cor.1:1991

ISO/IEC 10021-5/Cor.2:1991

ISO/IEC 10021-5/Cor.3:1992

ISO/IEC 10021-5/Cor.4:1992

ISO/IEC 10021-5/Cor.5:1992

Annex C

(informative)

Secure messaging - rationale and implementation considerations

C.1 Introduction

The purpose of the Security (SEC) functional group is to define an approach to the provision of secure messaging by Message Handling Systems (MHS) within the general framework of International Standardized Profiles for MHS.

C.2 Message handling vulnerabilities

The message handling vulnerabilities (threats) which can be protected using COMSEC and COMPUSEC measures are defined in annex D of ISO/IEC 10021-2:

- masquerade
- message sequencing
- modification of information
- denial of service
- repudiation
- leakage of information

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

- manipulation
- misrouting
- insider threats
- outsider threats

Some of these threats are defined in ISO 7498-2, which also specifies other threats, not all of which are relevant to MHS.

Annex D of ISO/IEC 10021-2 also indicates which MHS security services may provide protection against such threats. Some threats to MHS cannot be easily prevented, merely detected; others are not appropriate for standardization.

C.3 General principles

C.3.1 Security policy

A general **security policy** of an organization will stipulate which vulnerabilities are considered as threats and how these threats are countered (i.e., by procedural, physical, personnel, documentation and IT security measures). Such a 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 will need to cover all security aspects.

Security within an organization is not only the concern of MHS 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 vetting and confidence placed in staff), end-user access control, physical, procedural and documentation security. This annex is, however, only concerned with IT security, specifically in the areas of communications (COMSEC) and computer (COMPUSEC) security as applicable to standardization of a secure MHS operating in a store and forward environment.

C.3.2 Security classes

In the MHS base standards, some threats are countered by IT security measures. These measures are realized by providing security services and implemented using security elements.

This MHS ISP groups together those security features (services and elements) defined in the MHS base standards into an incremental set of **security classes**. A security class will not generally provide a complete realization of a security policy, but is rather intended as a generic component which can help to implement such a security policy.

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.

Each of the classes also has a variant (**SnC**) requiring support of end-to-end content confidentiality (the rationale for such variants is to avoid the implementation cost and processing overhead involved in encrypting the entire message content unless this is a definite requirement).

Each security class specifies a set of mandatory and optional security services. Mandatory security services within a security class can usually be selected by the subscriber or user, either on a per-message basis, or for an agreed contractual period of time. Although facilities and mechanisms to support mandatory security services must always be provided, it is a local issue to determine whether such a security service is offered for user selection or is permanently invoked. However, the use of some security services is always required for certain security classes. This is specified in this ISP by imposing additional dynamic requirements to those specified in the MHS base standards, ensuring that the corresponding protocol elements are always present. Similarly, use of some security services is prohibited for certain security classes. This is specified in this ISP by imposing additional dynamic requirements to those specified in the MHS base standards, ensuring that the protocol element is never present.

C.3.4 Encryption techniques

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

- symmetric encryption
- asymmetric encryption
- trusted functionality (i.e., COMPUSEC measures)

The MHS standards permit the use of the techniques on an individual basis to provide security services or they can be combined in line with a security policy. This ISP combines the techniques in order to provide a comprehensive set of security facilities, which are intended to counter the vulnerabilities of a messaging service. In some cases, the security services defined in the MHS standards can only be implemented using one of the techniques above, namely asymmetric encryption. However, the actual technique employed will be dependent on the algorithms, which will need to be registered by a security authority for the domain.

It is the intention of this ISP that implementations will not be restricted to asymmetric techniques. Wherever possible, the security services can be implemented using trusted functionality in combination with symmetric, asymmetric or both encryption techniques. In particular, this ISP permits the use of either asymmetric or symmetric techniques for both the signed and encrypted data within the message token.

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 must unambiguously identify the algorithm.

It is recommended that a conforming ASN.1 BIT STRING is normally used to contain the encrypted data (as generated by use of 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.

As defined in the MHS base standards, the ASN.1 Distinguished Encoded Rules must be used when the SIGNED, SIGNATURE or ENCRYPTED macros are required to implement secure messaging.

It is recommended that, in the absence of any requirement for support of other specific algorithms, implementations support the algorithms identified in 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, origin authentication checks), implementations should assume that all relevant data present in the subject message, probe or report has been included in the signature.

C.3.5 Implementation Issues

C.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 this ISP.

C.3.5.2 Confidentiality

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

Content Confidentiality may be achieved by either symmetric or asymmetric encryption techniques.

NOTE - Use of asymmetric techniques precludes submission of messages to multiple recipients that do not use the same secret key.

C.3.5.3 Integrity

Connection Integrity is provided using the underlying OSI layers and is outside the scope of this ISP. Mechanisms to support Connection Integrity are subject to bilateral agreement between peers. It should be noted that the integrity of a connection may 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 - i.e., by means of encrypted data in the message token (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 this ISP). 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/non-receipt notifications 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.

C.3.5.4 Message Origin Authentication

End-to-end (i.e., UA to UA) Message Origin Authentication (using the Message Argument Integrity security element) is automatically provided by Content Integrity. Security class S2 provides additional protection (i.e., of the integrity of the label) by requiring support of origin authentication checks within the MTS.

C.3.5.5 Proof/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-repudiation can be provided by the use of trusted accountability services.

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

C.3.5.6 Secure Access Management

Secure Access Management can be implemented by a combination of Multi-Level Security (MLS) functionality and assurance of the various MHS components to support such functionality. MLS functionality is supported in the MHS 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 MHS base standards and of this ISP. Reference should be made to the appropriate security authority and to any applicable security evaluation criteria (e.g., US DoD "Orange Book," European Information Technology Security Evaluation Criteria [ITSEC]).

The Security Context service ensures that a message security label matches at least one of the set of labels specified in the security context established between the communicating entities. An implementation which supports this service must as a minimum support exact matching for equality on the security-policy-identifier, security-classification and security-categories elements of the label. 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.

NOTE - The basic support requirement is that absence of an element is not treated as "any value" - i.e., all permissible combinations of occurrence and value for the elements of the message security label are elaborated in the security context. Thus, if a message with lesser protection requirements than the capabilities of the communicating entities is to be transferred, then it should be labelled with the appropriate security class identifier and the security context should include this class within the set of acceptable security-policy-identifiers. Interworking can even be restricted to messages of only one security class using this approach.

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 a message origin authentication check. Which of these labels is/are checked against the security context will depend on the security policy in force. The security policy should also define any requirements on allowable (per-recipient) label values in the case where a message is addressed to multiple recipients (and thus has multiple tokens). If a label is also included in the token encrypted data, then it should not have the same value as in the token signed data or the per-message extensions (and may thus have confidential end-to-end semantics). Such a label may be used for secure access management by the recipient UA.

C.3.5.7 Implications for the use of distribution lists

An MTA performing distribution list (DL) expansion must create all the per-recipient fields for the members of the DL. 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 should support at least the same security class as the originator and 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.

NOTE - If the security policy permits the use of distribution lists then it must also state the DL handling policy for notifications.

C.3.5.8 Implications for redirection

Implementation of the Security functional group may additionally either require that any redirection facilities are trusted, or alternatively prohibit the use of redirection altogether.

If the redirection facility is to be trusted, it will need to be subject to the security policy and obey the security labels as defined in the MHS base standards. It is recommended that the token is not altered on redirection (i.e., it should contain the originally-specified recipient name).

C.3.5.9 Implications for 84 interworking

Secure interworking between implementations conforming to the Security functional group and 1984 systems is not supported. The double enveloping technique can, however, be used to traverse a 1984 system.

C.3.5.10 Implications for use of the Directory

Implementation of the Security functional group may additionally either require that any Directory service used is trusted, or alternatively prohibit use of Directory services altogether.

C.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. For this reason, it is recommended that conversion prohibition is always set when non-secure MTAs are used for relay purposes.

C.3.5.12 Accountability

Accountability depends on the identification and authentication of users, and that all relevant information on the actions taken by users is properly recorded and stored.

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. Protocol-based mechanisms to support accountability will be subject to bilateral agreement.

C.3.5.13 Double enveloping

Double enveloping can be used with each security class as an optional extension to the security features which can be used to counter specific vulnerabilities. When double enveloping is used, it should be applied at the boundary of a domain and obey the rules of an MTA at management domain boundaries. Figure C.1 illustrates the technique.

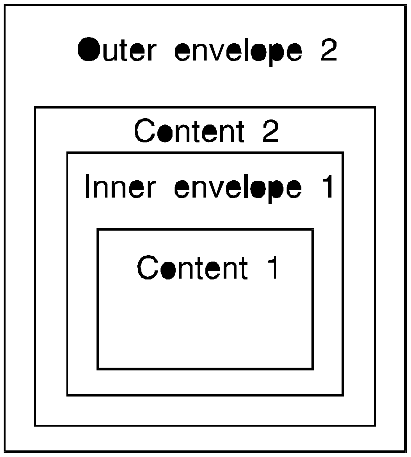


Figure C.1 - Double enveloping

The addressing and trace information in envelopes 1 and 2 are not necessarily the same. Trace information is not passed between the inner and outer envelopes. When the double enveloping technique is used, it is recommended that trace information on the outer envelope is always archived at the point where the inner envelope becomes the subject message.

The double enveloping technique can be used in 1988 and 1984 MTS environments and can in principle be applied on the submission, delivery or transfer envelopes. When used in a 1988 environment, any security class can be applied to the outer envelope 2. It is recommended that content 2 (inner envelope 1 plus content 1) is encrypted. When the double enveloping technique is used as a secure relay path via a 1984 domain, any encryption of content 2 will be subject to bilateral and/or multilateral agreement.

C.4 Security class S0

C.4.1 Rationale

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

- Content Integrity
- Message Origin Authentication (end-to-end)
- Proof of Delivery

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

C.4.2 Technical implications

The technical implications of security class S0 are as follows:

- an MTS-user will need mechanisms to generate the SIGNED, SIGNATURE and ENCRYPTED macros on message submission;
- an MTS-user will need mechanisms to handle the SIGNED, SIGNATURE and ENCRYPTED macros on message delivery.

C.5 Security class S1

C.5.1 Rationale

Security class S1 is a superset of security class S0 introducing basic requirements 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 trusting 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.

C.5.2 Technical implications

The technical implications of security class S1 are as for S0, plus:

- an MTA will need mechanisms to support registration, change-credentials and bind abstract operations (i.e., SIGNED macro for bind);
- an MS will need mechanisms to support MS-registration and the MS-bind operation (i.e., SIGNED macro for MS-Bind);
- message security labelling will need to be supported (the level of assurance is subject to individual security domain requirements);
- reliable access will need to be supported;
- an MTA will need to check the presence of security elements for which presence is specified as mandatory in this ISP;
- it will be necessary to provide a trusted OSI connection between peers, to provide adequate confidentiality, integrity and peer entity authentication.

C.6 Security class S2

C.6.1 Rationale

Security class S2 is a superset of security class S1. It requires MTAs 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 the MTS.

C.6.2 Technical implications

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

The technical implications of security class S2 are as for S1, plus:

- an MTA or MTS-user will need mechanisms to process the SIGNED macro of certificates, if certificates are used;
- the option of supporting Content Confidentiality cannot be allowed when the message origin authentication check (MOAC) is used to provide non-repudiation services;
- an MTA will need mechanisms to generate and process the SIGNATURE macro of message, probe and report authentication checks (MOAC, POAC and ROAC);
- an MTA or MTS-user will need mechanisms to interface with a Directory service supporting the Authentication Framework as defined in ISO/IEC 9594-8, or can otherwise distribute public keys by some other trusted means which is compliant with ISO/IEC 9594-8;
- it will be necessary to provide a trusted means of generating certificates, if certificates are used;

- an MTA will need mechanisms to generate a proof of submission SIGNATURE;
- an MTA will need mechanisms to generate ROAC SIGNATUREs with reports.

C.7 Confidential security class variants (SnC)

C.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.

C.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:

- an MTS-user will need mechanisms which can use the ENCRYPTED macro to encrypt and decrypt the message content.

Annex D

(informative)

Additional recommended practices for 1984 interworking

D.1 Introduction

This annex provides some additional recommendations concerning interworking between implementations conforming to ISO/IEC ISP 10611 (hereafter referred to as ‘1988 systems') and implementations conforming to earlier versions of the MHS base standards (hereafter referred to as ‘1984 systems').

Such recommendations are additional to the requirements of the 84 Interworking functional group, either because the interworking issue in question is outside the scope of the MHS base standards (and hence also outside the scope of formal conformance to this ISP) or because it is anticipated that the issue should be resolved in the MHS base standards.

D.2 Internal trace information

The interworking rules in annex B of ISO/IEC 10021-6 deal with most aspects of P1 downgrading, but do not cover MTAs which either generate or expect internal trace information as specified in the earlier draft MOTIS standard of 1985/6. Since the latter has now been superseded, the original specification is presented below for reference:

```
InternalTraceInfo       ::=   [APPLICATION 30] IMPLICIT SEQUENCE OF SEQUENCE {
                                    MTAName,
                                    MTASuppliedInfo }

MTAName                 ::=   PrintableString

MTASuppliedInfo         ::=   SET {
            arrival                 [0] IMPLICIT Time,
            deferred                [1] IMPLICIT Time OPTIONAL,
            action                        [2] IMPLICIT INTEGER {
                                          relayed                 (0),
                                          rerouted                (1),
                                          recipientReassignment   (2) }
            previous                MTAName OPTIONAL }
```

The following procedures provide a ‘mapping' or conversion between the standard internal trace information as supported by 1988 systems and internal trace information as specified above. They are recommended for use in those cases where it is required to support both 1988 systems and 1984 systems which support internal trace information to the above specification within the same domain.

The procedures are described in terms of the semantic changes required. It should, however, be noted that the ASN.1 syntax is also different and will require a complete translation.

D.2.1 Rules for transferring internal trace information to 1984 systems

If the global-domain-identifier of any internal-trace-information element does not identify the current domain, then that and all preceding internal-trace-information elements are deleted. The global-domain-identifier is deleted from all remaining internal-trace-information elements.

If converted-encoded-information-types is present in any internal-trace-information element, then that and all preceding internal-trace-information elements are deleted.

If any internal-trace-information element has either or both of the redirected and dl-operation bits of other-actions set, then an additional internal-trace-information element is generated by copying the MTA name and arrival elements and setting the action element to recipientReassignment (the new element is inserted immediately after the original element).

If any internal-trace-information element has an attempted element containing a domain, then that attempted element is deleted.

It should also be noted that the 1988 MHS base standards specify MTA name as IA5 String, whereas the 1984 internal trace information specification above uses Printable String. To avoid potential looping within a domain, it is recommended that MTA names only include those characters that are within the Printable String repertoire.

D.2.2 Rules for transferring internal trace information from 1984 systems

The global-domain-identifier of all internal-trace-information elements is set to identify the current domain.

If an internal-trace-information element is received from a 1984 system with an action value of recipientReassignment, then an other-actions element is generated with the redirected bit set. If the immediately preceding internal-trace-information element has an identical MTA name, then the generated other-actions element is added to it and the current internal-trace-information element is deleted. Otherwise, the current internal-trace-information element has the other-actions element added to it and the routing-action element is set to relayed.

D.3 Common-name O/R address attribute

[**Editor's Note :** The provisions of this clause are currently being balloted in the Sixth Proposed Technical Corrigendum to ISO/IEC 10021-6. If this is approved and referenced in this ISP then this clause can be deleted.]

The interworking rules in annex B of ISO/IEC 10021-6 only provide downgrading rules for P1 O/R address attributes which are encoded as Teletex String and make no reference to 1988 attributes which have no semantic equivalence in the 1984 standards. In view of the particular usefulness of the common-name O/R attribute to identify other than individual human MHS users, the following procedures have been defined to allow this attribute to be used by 1984 originators and to enable transfer across an intermediate 1984 domain. It is, however, emphasised that the procedures operate only on the P1 protocol when transferring between 1984 and 1988 MTAs.

When transferring to a 1984 MTA, if an O/R address contains the common-name (or teletex-common-name) extension attribute, then a domain-defined attribute is created with the type component set to "common" (not case sensitive) and the value component copied from the common-name attribute. The common-name attribute is then deleted. If the O/R address already contained four domain-defined attributes then downgrading of the O/R address fails.

When transferring from a 1984 MTA, if an O/R address contains a domain-defined attribute with the type component set to "common" (not case sensitive), then a common-name extension attribute is created with its value copied from the value component of that domain-defined attribute. That domain-defined attribute is then deleted.

NOTE - A teletex-common-name attribute can only be converted to a domain-defined attribute if the characters are drawn from the Printable String repertoire. When converting from a domain-defined attribute, the characters will always be drawn from the Printable String repertoire, but may be represented as either a common-name attribute or as a teletex-common-name attribute.

D.4 Other non-standard 1984 extensions

When responding to an incoming association establishment request from a 1984 system, the value of the protocol identifier should be accepted as either ‘1' or ‘8883'. When initiating an association establishment with a 1984 system, only the value ‘1' should be used for the protocol identifier.

Implementations may additionally support mapping of other non-standard 1984 extensions where there is an equivalent function in the 1988 standards (e.g., latest delivery designation), but should otherwise accept and discard such elements.

TITLE: Information technology - International Standardized Profiles AMH1n -
Message Handling Systems - Common Messaging -
Part 2 : Specification of ROSE, RTSE, ACSE, Presentation and Session Protocols for use by MHS

SOURCE: Project Editor (Jon Stranger, UK)

STATUS: DISP text, 1993-7-31

This document forms part of a proposed multipart ISP for MHS covering Common Messaging requirements (AMH1), as identified in the Taxonomy for International Standardized Profiles (ISO/IEC TR 10000-2 : 1992).

This revised DISP version reflects resolution of all remaining outstanding issues at the 6th MHS ISP Special Group (MISG) meeting (Kyoto, February 1-4, 1993) together with some editorial and minor errata which have been determined since submission to ISO/IEC JTC1/SGFS. The content of this document is considered by the MHS expert groups of the three regional workshops as harmonized.

The MHS-specific technical content of this document has been derived wherever possible from the existing EWOS/ETSI and OIW regional profiles in this area. The document also assumes the existence of an ISP covering Common Upper Layer Requirements (CULR), and references the current draft being developed jointly by the three regional workshops (Working Draft Version 11 of pDISP 11188-1, 1993-07-01). However, further changes to the draft CULR ISP may occur before publication as an ISP. In addition, pDISP 11188-1 does not cover ROSE or RTSE. A second part to pDISP 11188 covering the requirements of ROSE-based profiles is under development, but is not yet sufficiently mature for reference (and will still not cover RTSE). This document therefore references the CCITT RTSE and ROSE PICS proformas directly. As a result, although the content of this document is considered to be an internationally harmonized technical specification, the format and presentation may require further revision to align with the final CULR ISP.

Contents

Annexes

ISO/IEC Copyright Office _ Case Postale 56 _ CH-1211 Genève 20 _ Switzerland

Printed in Switzerland

Foreword

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

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC1. In addition to developing International Standards, ISO/IEC JTC1 has created a Special Group on Functional Standardization for the elaboration of International Standardized Profiles.

An International Standardized Profile is an internationally agreed, harmonized document which identifies a standard or group of standards, together with options and parameters, necessary to accomplish a function or set of functions.

Draft International Standardized Profiles are circulated to national bodies for voting. Publication as an International Standardized Profile requires approval by at least 75% of the national bodies casting a vote.

International Standardized Profile ISO/IEC ISP 10611-2 was prepared with the collaboration of:

- Asia-Oceania Workshop (AOW)

- European Workshop for Open Systems (EWOS) [jointly with the European Telecommunications Standards Institute (ETSI)]

- OSE Implementors' Workshop (OIW)

ISO/IEC ISP 10611 consists of the following parts, under the general title *Information technology - International Standardized Profiles AMH1n - Message Handling Systems - Common Messaging*:

- *Part 1 : MHS Service Support*

- *Part 2 : Specification of ROSE, RTSE, ACSE, Presentation and Session Protocols for use by MHS*

- *Part 3 : AMH11 - Message Transfer (P1)*

- *Part 4 : AMH12 - MTS Access (P3)*

- *Part 5 : AMH13 - MS Access (P7)*

This part of ISO/IEC ISP 10611 contains three annexes, A, B, and C, which are normative.

Introduction

This part of International Standardized Profile ISO/IEC ISP 10611 is defined within the context of Functional Standardization, in accordance with the principles specified by ISO/IEC TR 10000, “Framework and Taxonomy of International Standardized Profiles”. The context of Functional Standardization is one part of the overall field of Information Technology (IT) standardization activities, covering base standards, profiles, and registration mechanisms. A profile defines a combination of base standards that collectively perform a specific well-defined IT function. Profiles standardize the use of options and other variations in the base standards, and provide a basis for the development of uniform, internationally recognized system tests.

One of the most important rôles for an ISP is to serve as the basis for the development (by organizations other than ISO and IEC) of internationally recognized tests and test centres. ISPs are produced not simply to ‘legitimize' a particular choice of base standards and options, but to promote real system interoperability. The development and widespread acceptance of tests based on this and other ISPs is crucial to the successful realization of this goal.

The text for this part of ISO/IEC ISP 10611 was developed in close cooperation between the MHS Expert Groups of the three Regional Workshops: the North American OSE Implementors' Workshop (OIW), the European Workshop for Open Systems (EWOS) (jointly with the corresponding expert group of the European Telecommunications Standards Institute - ETSI) and the OSI Asia-Oceania Workshop (AOW). This part of ISO/IEC ISP 10611 is harmonized between these three Workshops and it has been ratified by the plenary assemblies of all three Workshops.

Information technology - International Standardized Profiles AMH1n - Message Handling Systems - Common Messaging

Part 2 : Specification of ROSE, RTSE, ACSE, Presentation and Session Protocols for use by MHS

1 Scope

1.1 General

This part of ISO/IEC ISP 10611 specifies how the Remote Operations Service Element, the Reliable Transfer Service Element, the Association Control Service Element, the Presentation Layer, and the Session Layer standards shall be used to provide the required OSI upper layer functions for MHS (see also figure 1). These specifications are therefore the common basis for the Common Messaging application functions, as defined in the other parts of ISO/IEC ISP 10611, and for content type-dependent International Standardized Profiles for MHS that will be developed.

1.2 Position within the taxonomy

This part of ISO/IEC ISP 10611 is the second part, as common text, of a multipart ISP identified in ISO/IEC TR 10000-2 as “AMH1, Message Handling Systems - Common Messaging” (see also ISO/IEC TR 10000-1, 8.2 for the definition of multipart ISPs).

This part of ISO/IEC ISP 10611 does not, on its own, specify any profiles.

1.3 Scenario

The model used is one of two end systems running an end-to-end association using either or both of RTSE and ROSE, and the ACSE, Presentation and Session services and protocols (see figure 1).

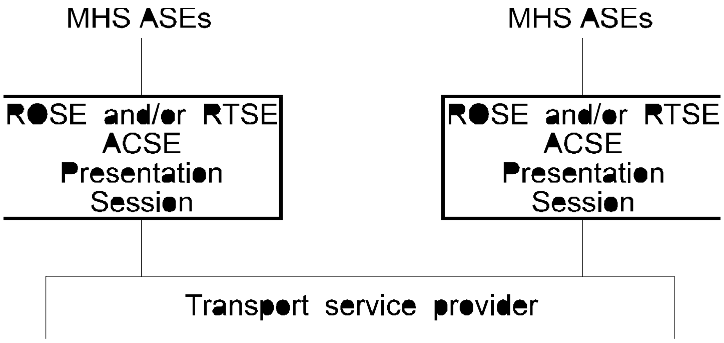


Figure 1 - Model of the supportive layers

The OSI upper layer services and protocols to support the Message Handling Systems functions covered by the

AMH1 set of profiles are specified in the set of standards identified in table 1.

Table 1 - AMH profile model

Application Layer	MHS	ISO/IEC 10021-6
	ROSE	ISO/IEC 9072-2
	RTSE	ISO/IEC 9066-2
	ACSE	see ISO/IEC ISP 11188-1
Presentation Layer		see ISO/IEC ISP 11188-1
Session Layer		see ISO/IEC ISP 11188-1

2 Normative references

The following documents contain provisions which, through reference in this text, constitute provisions of this part of ISO/IEC ISP 10611. At the time of publication, the editions indicated were valid. All documents are subject to revision, and parties to agreements based on this part of ISO/IEC ISP 10611 are warned against automatically applying any more recent editions of the documents listed below, since the nature of references made by ISPs to such documents is that they may be specific to a particular edition. Members of IEC and ISO maintain registers of currently valid International Standards and ISPs, and CCITT maintains published editions of its current Recommendations.

NOTE - References in the body of this part of ISO/IEC ISP 10611 to specific clauses of ISO/IEC documents shall be considered to refer also to the corresponding clauses of the equivalent CCITT Recommendations (as noted below) unless otherwise stated.

ISO/IEC 9066-2: 1989*, Information processing systems - Text Communication - Reliable Transfer - Part 2: Protocol specification.*

ISO/IEC 9072-2: 1989*, Information processing systems - Text Communication - Remote Operations - Part 2: Protocol specification.*

ISO/IEC TR 10000-1: 1992*, Information technology - Framework and taxonomy of International Standardized Profiles - Part 1: Framework.*

ISO/IEC TR 10000-2: 1992*, Information technology - Framework and taxonomy of International Standardized Profiles - Part 2: Taxonomy.*

ISO/IEC 10021-6: 1990*, Information technology - Text Communication - Message-Oriented Text Interchange Systems (MOTIS) - Part 6: Protocol Specifications. [see also CCITT Recommendation X.419(1988)]*

ISO/IEC ISP 11188-1: ---[2]*, Information technology - International Standardized Profiles - Common Upper Layer Requirements - Part 1: Basic connection oriented requirements.*

CCITT Recommendation X.248(1992)*, Reliable Transfer Service Element - Protocol Implementation Conformance Statement (PICS) Proforma.*

CCITT Recommendation X.249(1992)*, Remote Operations Service Element - Protocol Implementation Conformance Statement (PICS) Proforma.*

CCITT Recommendation X.419(1988)*, Message handling systems: Protocol specifications.*

[2] To be published.

3 Definitions

For the purposes of this part of ISO/IEC ISP 10611, the following definitions apply.

Terms used in this part of ISO/IEC ISP 10611 are as defined in the referenced base standards; in addition, the terms defined in ISO/IEC ISP 11188-1 apply.

4 Abbreviations

AC	Application context
ACSE	Association Control Service Element
AMH	Application Message Handling
ASN.1	Abstract Syntax Notation One
ISP	International Standardized Profile
MHS	Message Handling Systems
OSI	Open Systems Interconnection
PICS	Protocol Implementation Conformance Statement
ROSE	Remote Operations Service Element
RTSE	Reliable Transfer Service Element

Support level for protocol features:

m	mandatory support
o	optional support
c	conditional support
i	out of scope
–	not applicable

5 Conformance

This part of ISO/IEC ISP 10611 states requirements upon implementations to achieve interworking. A claim of conformance to this part of ISO/IEC ISP 10611 is a claim that all requirements in the relevant base standards are satisfied, that all the requirements in ISO/IEC ISP 11188-1 are satisfied, and that all requirements in the following clauses and in the annexes of this part of ISO/IEC ISP 10611 are satisfied. Annexes A, B and C state the relationship between these requirements and those of the base standards.

5.1 Conformance statement

The subsequent parts of ISO/IEC ISP 10611 specify the requirements for support of particular MHS application contexts. The requirements for conformance to this part of ISO/IEC ISP 10611 are as appropriate to the MHS application context(s) for which support is claimed, in accordance with ISO/IEC 10021-6.

For each implementation claiming conformance to this part of ISO/IEC ISP 10611 an appropriate set of PICSs shall be made available stating support or non-support of each option identified in this part of ISO/IEC ISP 10611.

5.2 Relationship with base standards

5.2.1 ROSE conformance

Implementations claiming support of any MHS application context which includes the Remote Operations Service Element (ROSE) shall implement all mandatory support (m) features (as specified in clause 6) unless those features are part of an unimplemented optional feature. They shall state which optional support (o) features are implemented.

5.2.2 RTSE conformance

Implementations claiming support of any MHS application context which includes the Reliable Transfer Service Element (RTSE) shall implement either or both of normal mode and X.410-1984 mode (as appropriate) and shall implement all mandatory support (m) features (as specified in clause 7) unless those features are part of an unimplemented optional feature. They shall state which optional support (o) features are implemented.

5.2.3 ACSE conformance

To conform to the Association Control Service Element (ACSE) protocol used in this part of ISO/IEC ISP 10611, implementations shall implement either or both of normal mode and X.410-1984 mode (as appropriate) and shall implement all mandatory support (m) features (as specified in clause 8) unless those features are part of an unimplemented optional feature. They shall state which optional support (o) features are implemented.

5.2.4 Presentation layer conformance

To conform to the Presentation protocol used in this part of ISO/IEC ISP 10611, implementations shall implement either or both of normal mode and X.410-1984 mode (as appropriate) and shall implement all mandatory support (m) features (as specified in clause 9) unless those features are part of an unimplemented optional feature. They shall state which optional support (o) features are implemented.

5.2.5 Transfer syntax conformance

Implementations conforming to this part of ISO/IEC ISP 10611 shall support the "Basic Encoding of a single ASN.1 type" as specified in ISO/IEC ISP 11188-1.

5.2.6 Session layer conformance

To conform to the Session protocol used in this part of ISO/IEC ISP 10611, implementations shall implement all mandatory support (m) features (as specified in clause 10) unless those features are part of an unimplemented optional feature. They shall state which optional support (o) features are implemented.

6 Remote Operations Service Element (ROSE)

The Remote Operations Service Element (ROSE) shall be supported for any P3 or P7 application context.

NOTE - P3 and P7 remote operations are Class 2 (asynchronous) operations.

The support of functions and parameters for ROSE is as specified in annex C of this part of ISO/IEC ISP 10611.

7 Reliable Transfer Service Element (RTSE)

The Reliable Transfer Service Element (RTSE) shall be supported for any P1 application context and for any P3 or P7 application context involving RTSE.

The support of functions and parameters for RTSE is as specified in annex B of this part of ISO/IEC ISP 10611 and as described below.

7.1 Dialogue-mode

Monologue dialogue-mode shall be supported for any P1 application context. In addition, two-way alternate dialogue-mode may optionally be supported.

Two-way alternate dialogue-mode shall be supported for any P3 or P7 application context involving RTSE.

In monologue dialogue-mode, the initiator shall keep the initial turn.

7.2 Checkpointing

Checkpointing shall be supported, both as initiator and as responder.

Use of no checkpointing without prior bilateral agreement on maximum APDU size is discouraged.

It shall be stated in the PICS which values of checkpoint size and window size are supported as initiator and as responder, and the maximum APDU size that can be supported in no checkpointing mode.

7.3 Mode

Normal mode shall be supported for the P1 mts-transfer application context and for any P3 or P7 application context. X.410-1984 mode shall be supported for the P1 mts-transfer-protocol and mts-transfer-protocol-1984 application contexts.

7.4 Elements of procedure

Support of checkpointing does not imply the capability to perform association recovery.

NOTE - It is recommended that the RTSE association recovery procedure (clause 7.8.3 of ISO/IEC 9066-2) is not used in a secure messaging environment, since the authentication of the RTSE association may be compromised (this is currently the subject of an RTSE defect report). It is permissible, however, to use the RTSE activity resumption procedure (clause 7.8.1 of ISO/IEC 9066-2) on an existing, authenticated, RTSE association.

8 Association Control Service Element (ACSE)

The support of functions and parameters for the Association Control Service Element is as specified in ISO/IEC ISP 11188-1 subject to any additional requirements in annex A of this part of ISO/IEC ISP 10611.

9 Presentation layer

The support of functions and parameters for the Presentation protocol is as specified in ISO/IEC ISP 11188-1 subject to any additional requirements in annex A of this part of ISO/IEC ISP 10611.

10 Session layer

The support of functions and parameters for the Session protocol is as specified in ISO/IEC ISP 11188-1 subject to any additional requirements in this clause and in annex A of this part of ISO/IEC ISP 10611.

10.1 Session version

Session version 2 shall be supported for the P1 mts-transfer application context and for any P3 or P7 application context. Session version 1 shall be supported for the P1 mts-transfer-protocol application context and for the P1 mts-transfer-protocol-1984 application context.

Any requirements with respect to which version(s) may be proposed for a particular association are as specified in the base standards, except that only version 1 shall be proposed for the P1 mts-transfer-protocol-1984 application context.

Annex A

(normative)

ISPICS Requirements List

Specific Upper Layer Requirements for ACSE, Presentation and Session

A.1 General

In the event of a discrepancy becoming apparent in the body of this part of ISO/IEC ISP 10611 and the tables in this annex, this annex is to take precedence.

The tables of this annex specify the level of support for the ACSE, Presentation and Session protocols, as required by the International Standardized Profiles AMHnn. Where features of these protocols are not specified in the tables of this annex then the requirements for conformance to this part of ISO/IEC ISP 10611 are as specified in the corresponding annex of ISO/IEC ISP 11188-1. The notation used for references is as specified in clause A.2 of pDISP 11188-1.

[**Editor's Note** : The structure and format of this annex may need to be revised to align with the final text of ISO/IEC ISP 11188-1 when this is achieved, but no technical changes are anticipated.]

A.2 Classification of requirements

In each table, the "Base" column reflects the level of support required for conformance to the base standard and the "Profile" column reflects the level of support required by this ISP. The specification of levels of support uses the classification defined in clause 3 of ISO/IEC ISP 11188-1.

A.3 Association Control Service Element

A.3.1 Supported rôles

A.3.1.1 Association establishment

Ref	Capability	Base	Profile
A.A.5.1/1	Association initiator	o	c1
A.A.5.1/2	Association responder	o	c2

c1 - if any P1 or P3 AC is supported, or if any P7 AC is supported by a UA, then m else i

c2 - if any P1 or P3 AC is supported, or if any P7 AC is supported by an MS, then m else i

A.3.2 Protocol mechanisms

Ref	Protocol Mechanism	Base	Profile
A.A.6/1	Normal mode	o	c1
A.A.6/2	X.410-1984 mode	o	c2
A.A.6/4	Supports operation of Session version 2	o	c1

c1 - if only the P1 **mts-transfer-protocol** and/or P1 **mts-transfer-protocol-1984** AC is supported then o else m

c2 - if the P1 **mts-transfer-protocol** and/or P1 **mts-transfer-protocol-1984** AC is supported then m else –

A.3.3 Supported APDU parameters

A.3.3.1 A-associate-request (AARQ)

Ref	Protocol Mechanism	Base	Profile
A.A.9.1/15	User information	o	m

A.3.3.2 A-associate-response (AARE)

Ref	Protocol Mechanism	Base	Profile
A.A.9.2/13	User information	o	m

A.3.3.3 A-release-request (RLRQ)

Ref	Protocol Mechanism	Base	Profile
A.A.9.3/2	User information	o	m

A.3.3.4 A-release-response (RLRE)

Ref	Protocol Mechanism	Base	Profile
A.A.9.4/2	User information	o	m

A.4 Presentation protocol

A.4.1 Functional units

Ref	Presentation functional unit	Base	Profile
P.A.5.2/2	Presentation Context Management	o	i
P.A.5.2/3	Presentation Context Restoration	c1	i

c1 - if Presentation Context Management (2) is supported then o else –

A.5 Session protocol

A.5.1 Protocol versions implemented

Ref	Version	Base	Profile
S.A.3/1	Version 1	o	c1
S.A.3/2	Version 2	o	c2

c1 - if the P1 **mts-transfer-protocol** and/or P1 **mts-transfer-protocol-1984** AC is supported then m else o

c2 - if only the P1 **mts-transfer-protocol** and/or P1 **mts-transfer-protocol-1984** AC is supported then o else m

A.5.2 Functional units

Ref	Functional unit	Base	Profile
S.A.6.1/3	Half Duplex	o	c2
S.A.6.1/4	Duplex	o	c3
S.A.6.1/8	Minor Synchronize	o	c2
S.A.6.1/12	Exceptions	c1	c2
S.A.6.1/13	Activity Management	o	c2

c1 - if Half Duplex (3) is supported then o else –

c2 - if RTSE is included in any supported AC then m else i

c3 - if a supported AC includes ROSE but not RTSE then m else –

A.5.3 Protocol mechanisms

Ref	Mechanism	Base	Profile
S.A.6.2/1	Use of transport expedited data	o	i
S.A.6.2/6	Segmenting (sending)	o	i
S.A.6.2/7	Segmenting (receiving)	o	i

Annex B

(normative)

ISPICS Requirements List for RTSE

B.1 General

In the event of a discrepancy becoming apparent in the body of this part of ISO/IEC ISP 10611 and the tables in this annex, this annex is to take precedence.

The tables of this annex specify the level of support for the RTSE protocol, as required by the International Standardized Profiles AMHnn, as a set of constraints and characteristics on what shall or may appear in the implementation columns of an ISPICS. This annex is completely based on CCITT Recommendation X.248(1992). It uses only a selection of the tables from that Recommendation which are necessary for the specification of ISP requirements (references indicate the clause containing the corresponding table and the row number within that table where applicable). Where features of this protocol are not specified in the tables of this annex then the requirements for conformance to this part of ISO/IEC ISP 10611 are as specified in CCITT Recommendation X.248(1992).

In each table, the "Base" column reflects the level of support required for conformance to the base standard and the "Profile" column reflects the level of support required by this ISP. The specification of levels of support uses the classification defined in clause 3 of ISO/IEC ISP 11188-1.

B.2 Initiator/responder capability

Ref	Capability	Base	Profile
A.6.1/1	Initiator	o	c1
A.6.1/2	Responder	o	c2

c1 - if any P1 or reliable P3 AC is supported, or if any reliable P7 AC is supported by a UA, then m else i

c2 - if any P1 or reliable P3 AC is supported, or if any reliable P7 AC is supported by an MS, then m else i

B.3 Major capabilities

B.3.1 Protocol mechanisms

Ref	Protocol Mechanism	Base	Profile
A.6.2.1/1	Normal mode	o	c1
A.6.2.1/2	X.410-1984 mode	o	c2

c1 - if the P1 **mts-transfer** AC and/or any reliable P3 or P7 AC is supported then m else o

c2 - if the P1 **mts-transfer-protocol** and/or P1 **mts-transfer-protocol-1984** AC is supported then m else –

B.3.2 Dialogue mode

Ref	Capability	Base	Profile
A.6.2.2	Monologue dialogue-mode	o	c1
A.6.2.2	Two-way alternate dialogue-mode	o	c2

c1 - if any P1 AC is supported then m else –

c2 - if any reliable P3 or P7 AC is supported then m else o

B.4 Additional information

The following table shall be completed to indicate the operational capabilities of the implementation.

Ref	Capability	Value/range of values
1	Maximum APDU size supported in no checkpointing mode	

Annex C

(normative)

ISPICS Requirements List for ROSE

C.1 General

In the event of a discrepancy becoming apparent in the body of this part of ISO/IEC ISP 10611 and the tables in this annex, this annex is to take precedence.

The tables of this annex specify the level of support for the ROSE protocol, as required by the International Standardized Profiles AMHnn, as a set of constraints and characteristics on what shall or may appear in the implementation columns of an ISPICS. This annex is completely based on CCITT Recommendation X.249(1992). It uses only a selection of the tables from that Recommendation which are necessary for the specification of ISP requirements (references indicate the clause containing the corresponding table and the row number within that table where applicable). Where features of this protocol are not specified in the tables of this annex then the requirements for conformance to this part of ISO/IEC ISP 10611 are as specified in CCITT Recommendation X.249(1992).

In each table, the "Base" column reflects the level of support required for conformance to the base standard and the "Profile" column reflects the level of support required by this ISP. The specification of levels of support uses the classification defined in clause 3 of ISO/IEC ISP 11188-1.

C.2 Application entity requirements

Ref	Protocol Mechanism	Base	Profile
A.6.1/2	Is Operation Class 2 supported?	o	m
A.6.1/6	Is the ROSE a component of an application entity that invokes operations?	o	m
A.6.1/7	Is the ROSE a component of an application entity that performs operations?	o	m

TITLE: Information technology - International Standardized Profiles AMH1n -
Message Handling Systems - Common Messaging -
Part 3 : AMH11 - Message Transfer (P1)

SOURCE: Project Editor (Jon Stranger, UK)

STATUS: DISP text, 1993-7-31

This document forms part of a proposed multipart ISP for MHS covering Common Messaging requirements (AMH1), as identified in the Taxonomy for International Standardized Profiles (ISO/IEC TR 10000-2 : 1992).

This revised DISP version reflects resolution of all remaining outstanding issues at the 6th MHS ISP Special Group (MISG) meeting (Kyoto, February 1-4, 1993) together with some editorial and minor errata which have been determined since submission to ISO/IEC JTC1/SGFS. The content of this document is considered by the MHS expert groups of the three regional workshops as harmonized.

The technical content of this document has been derived wherever possible from the existing EWOS/ETSI and OIW regional profiles in this area. However, differences between the content of this document and one or more regional profiles may exist.

Contents

Annexes

ISO/IEC Copyright Office _ Case Postale 56 _ CH-1211 Genève 20 _ Switzerland

Printed in Switzerland

Foreword

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

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC1. In addition to developing International Standards, ISO/IEC JTC1 has created a Special Group on Functional Standardization for the elaboration of International Standardized Profiles.

An International Standardized Profile is an internationally agreed, harmonized document which identifies a standard or group of standards, together with options and parameters, necessary to accomplish a function or set of functions.

Draft International Standardized Profiles are circulated to national bodies for voting. Publication as an International Standardized Profile requires approval by at least 75% of the national bodies casting a vote.

International Standardized Profile ISO/IEC ISP 10611-3 was prepared with the collaboration of:

- Asia-Oceania Workshop (AOW)

- European Workshop for Open Systems (EWOS) [jointly with the European Telecommunications Standards Institute (ETSI)]

- OSE Implementors' Workshop (OIW)

ISO/IEC ISP 10611 consists of the following parts, under the general title *Information technology - International Standardized Profiles AMH1n - Message Handling Systems - Common Messaging*:

- *Part 1 : MHS Service Support*

- *Part 2 : Specification of ROSE, RTSE, ACSE, Presentation and Session Protocols for use by MHS*

- *Part 3 : AMH11 - Message Transfer (P1)*

- *Part 4 : AMH12 - MTS Access (P3)*

- *Part 5 : AMH13 - MS Access (P7)*

This part of ISO/IEC ISP 10611 contains two annexes, A and B, which are normative.

Introduction

This part of International Standardized Profile ISO/IEC ISP 10611 is defined within the context of Functional Standardization, in accordance with the principles specified by ISO/IEC TR 10000, “Framework and Taxonomy of International Standardized Profiles”. The context of Functional Standardization is one part of the overall field of Information Technology (IT) standardization activities, covering base standards, profiles, and registration mechanisms. A profile defines a combination of base standards that collectively perform a specific well-defined IT function. Profiles standardize the use of options and other variations in the base standards, and provide a basis for the development of uniform, internationally recognized system tests.

One of the most important rôles for an ISP is to serve as the basis for the development (by organizations other than ISO and IEC) of internationally recognized tests and test centres. ISPs are produced not simply to ‘legitimize' a particular choice of base standards and options, but to promote real system interoperability. The development and widespread acceptance of tests based on this and other ISPs is crucial to the successful realization of this goal.

The text for this part of ISO/IEC ISP 10611 was developed in close cooperation between the MHS Expert Groups of the three Regional Workshops: the North American OSE Implementors' Workshop (OIW), the European Workshop for Open Systems (EWOS) (jointly with the corresponding expert group of the European Telecommunications Standards Institute - ETSI) and the OSI Asia-Oceania Workshop (AOW). This part of ISO/IEC ISP 10611 is harmonized between these three Workshops and it has been ratified by the plenary assemblies of all three Workshops.

Information technology - International Standardized Profiles AMH1n - Message Handling Systems - Common Messaging

Part 3 : AMH11 - Message Transfer (P1)

1 Scope

1.1 General

This part of ISO/IEC ISP 10611 (AMH11) covers message transfer between message transfer agents (MTAs) using the P1 Message Transfer Protocol (see also figure 1). These specifications form part of the Common Messaging application functions, as defined in the parts of ISO/IEC ISP 10611, which form a common basis for content type-dependent International Standardized Profiles for MHS that will be developed.

An MTA which conforms to profiles AMH11n as specified in this part of ISO/IEC ISP 10611 may support a 'normal mode' OSI protocol infrastructure as required by ISO/IEC 10021-6 (AMH111), and/or support an 'X.410 mode' OSI protocol infrastructure as required by the CCITT X.400(1988) Recommendations (AMH112).

NOTE - An MTA which only supports the minimum requirements of AMH111 will not interwork with an MTA which only supports the minimum requirements of AMH112.

1.2 Position within the taxonomy

This part of ISO/IEC ISP 10611 is the third part of a multipart ISP identified in ISO/IEC TR 10000-2 as "AMH1, Message Handling Systems - Common Messaging" (see also ISO/IEC TR 10000-1, 8.2 for the definition of multipart ISPs).

This part of ISO/IEC ISP 10611 specifies the following profiles:

AMH111 - Message Transfer (P1) - Normal mode

AMH112 - Message Transfer (P1) - X.410(1984) mode

The AMH11n profiles may be combined with any T-Profiles (see ISO/IEC TR 10000) specifying the OSI connection-mode Transport service.

1.3 Scenario

The model used is one of two or more MTAs intercommunicating within a Message Transfer System (MTS) using the P1 protocol, as shown in figure 1.

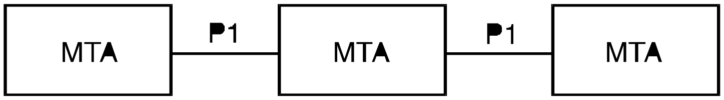


Figure 1 - AMH11n scenario

The AMH11n profiles cover all aspects of the MTA Abstract Service, as defined in clause 12 of ISO/IEC 10021-4, when realized using the P1 protocol.

The OSI upper layer services and protocols to support the Message Handling Systems functions covered by the AMH11n profiles are specified in the set of standards identified in table 1.

Table 1 - AMH11n profile model

Application Layer	MHS	ISO/IEC 10021-6
	RTSE	see ISO/IEC ISP 10611-2
	ACSE	see ISO/IEC ISP 10611-2
Presentation Layer		see ISO/IEC ISP 10611-2
Session Layer		see ISO/IEC ISP 10611-2

2 Normative references

The following documents contain provisions which, through reference in this text, constitute provisions of this part of ISO/IEC ISP 10611. At the time of publication, the editions indicated were valid. All documents are subject to revision, and parties to agreements based on this part of ISO/IEC ISP 10611 are warned against automatically applying any more recent editions of the documents listed below, since the nature of references made by ISPs to such documents is that they may be specific to a particular edition. Members of IEC and ISO maintain registers of currently valid International Standards and ISPs, and CCITT maintains published editions of its current Recommendations.

Amendments and corrigenda to the base standards referenced are listed in annex B.

NOTE - References in the body of this part of ISO/IEC ISP 10611 to specific clauses of ISO/IEC documents shall be considered to refer also to the corresponding clauses of the equivalent CCITT Recommendations (as noted below) unless otherwise stated.

ISO/IEC TR 10000-1: 1992, *Information technology - Framework and taxonomy of International Standardized Profiles - Part 1: Framework.*

ISO/IEC TR 10000-2: 1992, *Information technology - Framework and taxonomy of International Standardized Profiles - Part 2: Taxonomy.*

ISO/IEC 10021-1: 1990, *Information technology - Text Communication - Message-Oriented Text Interchange Systems (MOTIS) - Part 1: Service Overview. [see also CCITT Recommendation X.400(1988)]*

ISO/IEC 10021-2: 1990, *Information technology - Text Communication - Message-Oriented Text Interchange Systems (MOTIS) - Part 2: Overall Architecture. [see also CCITT Recommendation X.402(1988)]*

ISO/IEC 10021-4: 1990, *Information technology - Text Communication - Message-Oriented Text Interchange Systems (MOTIS) - Part 4: Message Transfer System: Abstract Service Definition and Procedures. [see also CCITT Recommendation X.411(1988)]*

ISO/IEC 10021-6: 1990, *Information technology - Text Communication - Message-Oriented Text Interchange Systems (MOTIS) - Part 6: Protocol Specifications. [see also CCITT Recommendation X.419(1988)]*

ISO/IEC ISP 10611-1: ---[3], *Information technology - International Standardized Profiles AMH1n - Message Handling Systems -*

[3] To be published.

Common Messaging - Part 1: MHS Service Support.

ISO/IEC ISP 10611-2: ---[1], *Information technology - International Standardized Profiles AMH1n - Message Handling Systems - Common Messaging - Part 2: Specification of ROSE, RTSE, ACSE, Presentation and Session Protocols for use by 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.411(1988)*, Message handling systems: Message transfer system: Abstract service definition and procedures.*

CCITT Recommendation X.419(1988)*, Message handling systems: Protocol specifications.*

MHS Implementors' Guide, Version 8, March 1992 (CCITT Special Rapporteur's Group on Message Handling Systems and ISO/IEC JTC1/SC18/WG4 SWG on Messaging).

3 Definitions

For the purposes of this part of ISO/IEC ISP 10611, the following definitions apply.

Terms used in this part of ISO/IEC ISP 10611 are defined in the referenced base standards; in addition, the following terms are defined.

3.1 General

Basic requirement : an Element of Service, protocol element, procedural element or other identifiable feature specified in the base standards which is required to be supported by all MHS implementations.

Functional group : a specification of one or more related Elements of Service, protocol elements, procedural elements or other identifiable features specified in the base standards which together support a significant optional area of MHS functionality.

NOTE - A functional group can cover any combination of MHS features specified in the base standards for which the effect of implementation can be determined at a standardized external interface - i.e., via a standard OSI communications protocol (other forms of exposed interface, such as a standardized programmatic interface, are outside the scope of this version of ISO/IEC ISP 10611).

3.2 Support classification

To specify the support level of arguments, results and other protocol features for this part of ISO/IEC ISP 10611, the following terminology is defined.

3.2.1 Static capability

The following classifications are used in this part of ISO/IEC ISP 10611 to specify static conformance requirements - i.e., capability.

In the case of protocol elements, the classification is relative to that of the containing element, if any. Where the constituent elements of a non-primitive element are not individually specified, then each shall be considered to have the classification of that element. Where the range of values to be supported for an element is not specified, then all values defined in the MHS base standards shall be supported.

mandatory full support (**m**) : the element or feature shall be fully supported. An implementation shall be able to generate the element, and/or receive the element and perform all associated procedures (i.e., implying the ability to handle both the syntax and the semantics of the element) as relevant, as specified in the MHS base standards. The receiving capability shall be considered to include relaying where appropriate. Where support for origination (generation) and reception are not distinguished, then both capabilities shall be assumed.

mandatory minimal support (**m-**) : the element shall be supported. However, an implementation is only required to be able to copy the syntax of the element to the corresponding element of a message, probe or report for onward transfer or delivery, as appropriate, according to the procedures as specified in the MHS base standards, unless further qualified for the output envelope in question elsewhere in this ISP (i.e., the classification of the output envelope takes precedence). An implementation is not required to be able to take any explicit action based on the semantics of such an element other than to obey criticality. An implementation is not required to be able to originate such an element.

NOTE - The m- classification is designed to distinguish those cases where the MHS base standards define more than one level of functionality and the minimum required level of support in this profile is the minimum functionality defined in the base standards. Where the only functionality defined in the base standards is copying the element as described above, then the m classification is used in preference to m-.

optional support (**o**) : an implementation is not required to support the element. If support is claimed, the element shall be treated as if it were specified as mandatory support. If support is not claimed, and the element is an argument, then an implementation shall generate an appropriate error if the element is received. If support is not claimed, and the element is a result, then an implementation may ignore the element if it is received.

conditional support (**c**) : the element shall be supported under the conditions specified in this part of ISO/IEC ISP 10611. If these conditions are met, the element shall be treated as if it were specified as mandatory support. If these conditions are not met, the element shall be treated as if it were specified as optional support (unless otherwise stated).

out of scope (**i**) : the element is outside the scope of this part of ISO/IEC ISP 10611 - i.e., it will not be the subject of an ISP conformance test.

not applicable (**–**) : the element is not applicable in the particular context in which this classification is used.

3.2.2 Dynamic behaviour

The above classifications are used in this part of ISO/IEC ISP 10611 to specify static conformance requirements (i.e., capability); dynamic conformance requirements (i.e., behaviour) are as specified in the MHS base standards. However, in a few cases it has been necessary to specify additional dynamic conformance requirements in this profile. These are specified using a second classification code for an element, as follows.

NOTE - Clause 6.7 of ISO/IEC TR 10000-1 states that a profile shall not introduce a constraint on dynamic behaviour on reception. However, in the case of MHS security (at least), the base standards define a suitable error indication to cover the breach of a security policy but do not specify the precise conditions under which such error indication shall be used. Any such specification in a profile is thus a legitimate qualification of the base standards rather than a modification of such provisions.

required (**r**) : the element shall always be present. An implementation shall ensure that the element is always generated or otherwise used, as appropriate. Absence of the element on reception shall result in termination or rejection of the communication with an appropriate error indication as specified in the MHS base standards.

excluded (**x**) : the element shall never be present. An implementation shall ensure that the element is never generated or otherwise used, as appropriate. Presence of the element on reception shall result in termination or rejection of the communication with an appropriate error indication as specified in the MHS base standards.

NOTE - It is recognized that some implementations may be required to exclude even a static capability in such cases, but such considerations are outside the scope of this profile. Any elements which are specified as excluded (x) in this profile are thus also specified as out of scope (i) in terms of static capability.

4 Abbreviations

84IW	84 Interworking
AMH	Application Message Handling
ASN.1	Abstract Syntax Notation One
CV	Conversion
DIR	Use of Directory
DL	Distribution List
EoS	Element of Service
FG	Functional group
ISP	International Standardized Profile
LD	Latest Delivery
MHS	Message Handling Systems
MS	Message store
MTA	Message transfer agent
OSI	Open Systems Interconnection
PD	Physical Delivery
PDAU	Physical delivery access unit
RED	Redirection
RoC	Return of Contents
SEC	Security
UA	User agent

Support level for protocol elements and features (see 3.2):

m	mandatory full support
m-	mandatory minimal support
o	optional support
c	conditional support
i	out of scope
–	not applicable
r	required
x	excluded

5 Conformance

This part of ISO/IEC ISP 10611 states requirements upon implementations to achieve interworking. A claim of conformance to this part of ISO/IEC ISP 10611 is a claim that all requirements in the relevant base standards are satisfied, and that all requirements in the following clauses and in annex A of this part of ISO/IEC ISP 10611 are satisfied. Annex A states the relationship between these requirements and those of the base standards.

5.1 Conformance statement

For each implementation claiming conformance to profiles AMH11n as specified in this part of ISO/IEC ISP 10611, a PICS shall be made available stating support or non-support of each option identified in this part of ISO/IEC ISP 10611.

The scope of conformance to profiles AMH11n is restricted to MTAs. A claim of conformance to profiles AMH11n shall state whether the implementation supports profile AMH111 and/or profile AMH112 (jointly referenced as AMH11 in this part of ISO/IEC ISP 10611 where a distinction is unnecessary).

5.2 MHS conformance

This part of ISO/IEC ISP 10611 specifies implementation options or selections such that conformant implementations will satisfy the conformance requirements of ISO/IEC 10021 and/or the CCITT X.400 Recommendations.

NOTE - The ISO/IEC and CCITT conformance requirements currently differ with respect to support of P1 application contexts, as described in annex D of ISO/IEC 10021-6 and CCITT Recommendation X.419(1988). However, the 1992 CCITT X.400 Recommendations will require support of all P1 application contexts.

Implementations conforming to profile AMH11 as specified in this part of ISO/IEC ISP 10611 shall implement all the mandatory support (m or m-) features identified as basic requirements in annex A and shall state which optional support (o) features are implemented. They shall also support corresponding MHS Elements of Service and associated procedures as specified in ISO/IEC ISP 10611-1, as appropriate to the scope of this profile.

Implementations conforming to profile AMH11 as specified in this part of ISO/IEC ISP 10611 shall state whether or not they support any of the optional functional groups as specified in ISO/IEC ISP 10611-1 which are applicable to the scope of this profile. Implementations conforming to profile AMH112 shall support the 84 Interworking functional group. For each functional group for which support is claimed, an implementation shall implement all the mandatory support (m or m-) features identified for that functional group in annex A and shall state which optional support (o) features are implemented. They shall also support corresponding MHS Elements of Service and associated procedures as specified in ISO/IEC ISP 10611-1, as appropriate to the scope of this profile.

Implementations conforming to profile AMH11 as specified in this part of ISO/IEC ISP 10611 shall state the P1 application context(s) for which conformance is claimed. Implementations conforming to profile AMH111 shall support the P1 mts-transfer application context. Implementations conforming to profile AMH112 shall support the P1 mts-transfer-protocol and mts-transfer-protocol-1984 application contexts. Implementations conforming to profile AMH111 which also support the P1 mts-transfer-protocol-1984 application context shall support the 84 Interworking functional group.

5.3 Underlying layers conformance

Implementations conforming to profile AMH11 as specified in this part of ISO/IEC ISP 10611 shall also conform to ISO/IEC ISP 10611-2 in accordance with the P1 application context(s) for which conformance is claimed.

Annex A[1]

(normative)

ISPICS Proforma

for ISO/IEC ISP 10611-3 (AMH11)

In the event of a discrepancy becoming apparent in the body of this part of ISO/IEC ISP 10611 and the tables in this annex, this annex is to take precedence.

[**Editor's Note** : It had been intended that this annex would eventually be based on the ISO/IEC 10021 P1 PICS proforma. However, the current version of the latter (as contained in ISO/IEC CD 10021-12) is defective and the whole ISO/IEC work item for the development of MOTIS PICS proformas has now been suspended. As a result, it has been necessary to turn the P1 IPRL in this annex into a complete ISPICS proforma (the alternative approach of a separate annex containing the assumed base standard PICS proforma was not considered appropriate in this case). This annex broadly follows the final draft of CCITT Recommendation X.482 (April 1992), but the structure has been modified to some extent to take account of profiling requirements and the somewhat different conformance objectives.]

Clause A.1 specifies the basic requirements for conformance to profile AMH11. Clause A.2 specifies additional requirements to those specified in A.1 for each of the optional functional groups if conformance to such a functional group is claimed. Clause A.3 allows additional information to be provided for certain aspects of an implementation where no specific requirements are included in ISO/IEC ISP 10611. All three clauses shall be completed as appropriate.

In each table, the "Base" column reflects the level of support required for conformance to the base standard and the "Profile" column specifies the level of support required by this ISP (using the classification and notation defined in 3.2).

[**Editor's Note** : The identification of the base standard requirement has in some cases had to be interpreted or varied from that specified in the current CCITT PICS proforma, either due to the different classification scheme employed or where the base standard is unclear and it has been considered that the CCITT PICS proforma is in error.]

The Support column is provided for completion by the supplier of the implementation as follows:

Y	the element or feature is fully supported (i.e., satisfying the requirements of the m profile support classification)
Y-	the element or feature is minimally supported (i.e., satisfying the requirements of the m- profile support classification)
N	the element or feature is not supported, further qualified to indicate the action taken on

[1] **Copyright release for ISPICS proformas**
Users of this International Standardized Profile may freely reproduce the ISPICS proforma in this annex so that it can be used for its intended purpose and may further publish the completed ISPICS.

receipt of such an element as follows:

ND - the element is discarded/ignored
NR - the PDU is rejected (with an appropriate error indication where applicable)

– or blank the element or feature is not applicable (i.e., a major feature or composite protocol element which includes this element or feature is not supported)

Identification of the implementation

Identification of PICS

Ref	Question	Response
1	Date of statement (DD/MM/YY)	
2	PICS serial number	
3	System conformance statement cross reference	

Identification of IUT

Ref	Question	Response
1	Implementation name	
2	Implementation version	
3	Machine name	
4	Machine version	
5	Operating system name	
6	Operating system version	
7	Special configuration	
8	Other information	

Identification of supplier

Ref	Question	Response
1	Organization name	
2	Contact name(s)	
3	Address	
4	Telephone number	
5	Telex number	
6	Fax number	
7	E-mail address	
8	Other information	

Identification of protocol

Ref	Question	Response
1	Title, reference number and date of publication of the protocol standard	
2	Protocol version(s)	
3	Addenda/amendments/corrigenda implemented	
4	Defect reports implemented	

Global statement of conformance

Ref	Question	Response	Comments
1	Are all mandatory base standards requirements implemented?		

Statement of profile conformance

Ref	Question	Response	Comments
1	Are all mandatory requirements of profile AMH111 implemented?		
2	Are all mandatory requirements of profile AMH112 implemented?		
3	Are all mandatory requirements of any of the following optional functional groups implemented?		
3.1	Security (SEC)		class(es):
3.2	Physical Delivery (PD)		
3.3	Conversion (CV)		
3.4	Redirection (RED)		
3.5	Latest Delivery (LD)		
3.6	Return of Contents (RoC)		
3.7	Distribution List (DL)		
3.8	Use of Directory (DIR)		
3.9	84 Interworking (84IW)		

A.1 Basic requirements

A.1.1 Initiator/responder capability

Ref	Application Context	Base		Profile	Support
		CCITT	ISO/IEC		
1	Initiator	m	m	m	
2	Responder	m	m	m	

A.1.2 Supported application contexts

Ref	Application Context	Base		Profile	Support
		CCITT	ISO/IEC		
1	mts-transfer	o	m	c1	
2	mts-transfer-protocol	m	o	c2	
3	mts-transfer-protocol-1984	m	o	c2	

c1 - if conformance to AMH111 is claimed then m else o

c2 - if conformance to AMH112 is claimed then m else o

A.1.3 PDUs and operations

A.1.3.1 PDUs

Ref	PDU	Base	Profile	Support	Notes/References
1	message	m	m		see A.1.4.2
2	report	m	m		see A.1.4.3
3	probe	m	m		see A.1.4.4

A.1.3.2 Operations

Ref	Operation	Base	Profile	Support	Notes/References
1	MTA-bind	m	m		see A.1.4.1
2	MTA-unbind	m	m		

A.1.4 Operation arguments/results

A.1.4.1 MTA-bind

Ref	Element	Base	Profile	Support	Notes/References
1	ARGUMENT				
1.1	NULL	m	m		
1.2	SET	m	m		
1.2.1	initiator-name	m	m		
1.2.2	initiator-credentials	m	m		
1.2.2.1	simple	m	m		
1.2.2.1.1	OCTET STRING	o	m		
1.2.2.1.2	IA5String	o	c1		
1.2.2.2	strong	o	o		
1.2.2.2.1	bind-token	m	m		
1.2.2.2.1.1	signature-algorithm-identifier	m	m		
1.2.2.2.1.2	name	m	m		
1.2.2.2.1.3	time	m	m		
1.2.2.2.1.4	signed-data	o	o		

1.2.2.2.1.5	encryption-algorithm-identifier	o	o		
1.2.2.2.1.6	encrypted-data	o	o		
1.2.2.2.2	certificate	o	o		
1.2.3	security-context	o	o		see A.1.6/3
2	RESULT				
2.1	NULL	m	m		
2.2	SET	m	m		
2.2.1	responder-name	m	m		
2.2.2	responder-credentials	m	m		
2.2.2.1	simple	m	m		
2.2.2.1.1	OCTET STRING	o	m		
2.2.2.1.2	IA5String	o	c1		
2.2.2.2	strong	o	o		
2.2.2.2.1	bind-token	m	m		
2.2.2.2.1.1	signature-algorithm-identifier	m	m		
2.2.2.2.1.2	name	m	m		
2.2.2.2.1.3	time	m	m		
2.2.2.2.1.4	signed-data	o	o		
2.2.2.2.1.5	encryption-algorithm-identifier	o	o		
2.2.2.2.1.6	encrypted-data	o	o		

c1 - if the P1 **mts-transfer-protocol-1984** AC is supported then m else o

A.1.4.2 Message PDU parameters

Ref	Element	Base	Profile	Support	Notes/References
1	MessageTransferEnvelope	m	m		
1.1	(per message fields)				
1.1.1	message-identifier	m	m		see A.1.5/1
1.1.2	originator-name	m	m		see A.1.7
1.1.3	original-encoded-information-types	m	m-		see A.1.5/3
1.1.4	content-type	m	m-		see A.1.5/8
1.1.5	content-identifier	m	m		
1.1.6	priority	m	m		
1.1.7	per-message-indicators	m	m		see A.1.5/4
1.1.8	deferred-delivery-time	o	m-		
1.1.9	per-domain-bilateral-information	o	m-		see A.1.5/5
1.1.10	trace-information	m	m		see A.1.5/6
1.1.11	extensions				
1.1.11.1	recipient-reassignment-prohibited	o	m		
1.1.11.2	dl-expansion-prohibited	o	m		
1.1.11.3	conversion-with-loss-prohibited	o	m		
1.1.11.4	latest-delivery-time	o	m-		
1.1.11.5	originator-return-address	o	m-		see A.1.7
1.1.11.6	originator-certificate	o	m-		
1.1.11.7	content-confidentiality-algorithm-identifier	o	m-		
1.1.11.8	message-origin-authentication-check	o	m-		see A.1.6/2
1.1.11.9	message-security-label	o	m-		see A.1.6/3
1.1.11.10	content-correlator	m	m		
1.1.11.11	dl-expansion-history	m	m-		
1.1.11.12	internal-trace-information	m	m		see A.1.6/5
1.2	per-recipient-fields	m	m		
1.2.1	recipient-name	m	m		see A.1.7

1.2.2	originally-specified-recipient-number	m	m		
1.2.3	per-recipient-indicators	m	m		
1.2.4	explicit-conversion	o	m-		
1.2.5	extensions				
1.2.5.1	originator-requested-alternate-recipient	o	m-		see A.1.7
1.2.5.2	requested-delivery-method	o	m-		
1.2.5.3	physical-forwarding-prohibited	o	m-		
1.2.5.4	physical-forwarding-address-request	o	m-		
1.2.5.5	physical-delivery-modes	o	m-		
1.2.5.6	registered-mail-type	o	m-		
1.2.5.7	recipient-number-for-advice	o	m-		
1.2.5.8	physical-rendition-attributes	o	m-		
1.2.5.9	physical-delivery-report-request	o	m-		
1.2.5.10	message-token	o	m-		see A.1.6/4
1.2.5.11	content-integrity-check	o	m-		
1.2.5.12	proof-of-delivery-request	o	m-		
1.2.5.13	redirection-history	m	m-		
2	content	m	m		

A.1.4.3 Report PDU parameters

Ref	Element	Base	Profile	Support	Notes/References
1	ReportTransferEnvelope	m	m		
1.1	report-identifier	m	m		see A.1.5/1
1.2	report-destination-name	m	m		see A.1.7
1.3	trace-information	m	m		see A.1.5/6
1.4	extensions				
1.4.1	message-security-label	o	m-		see A.1.6/3
1.4.2	originator-and-DL-expansion-history	m	m		
1.4.3	reporting-DL-name	o	m-		see A.1.7
1.4.4	reporting-MTA-certificate	o	m-		
1.4.5	report-origin-authentication-check	o	m-		see A.1.6/8
1.4.6	internal-trace-information	m	m		see A.1.6/5
2	ReportTransferContent	m	m		
2.1.1	subject-identifier	m	m		see A.1.5/1
2.1.2	subject-intermediate-trace-information	o	m		see A.1.5/6
2.1.3	original-encoded-information-types	m	m		see A.1.5/3
2.1.4	content-type	m	m		see A.1.5/8
2.1.5	content-identifier	m	m		
2.1.6	returned-content	o	m-		
2.1.7	additional-information	o	m-		
2.1.8	extensions				
2.1.8.1	content-correlator	m	m		
2.2	per-recipient-fields	m	m		
2.2.1	actual-recipient-name	m	m		see A.1.7
2.2.2	originally-specified-recipient-number	m	m		
2.2.3	per-recipient-indicators	m	m		
2.2.4	last-trace-information	m	m		see A.1.5/7

2.2.5	originally-intended-recipient-name	m	m		see A.1.7
2.2.6	supplementary-information	o	m-		
2.2.7	extensions				
2.2.7.1	redirection-history	m	m		
2.2.7.2	physical-forwarding-address	o	m-		see A.1.7
2.2.7.3	recipient-certificate	o	m-		
2.2.7.4	proof-of-delivery	o	m-		see A.1.6/7

A.1.4.4 Probe PDU parameters

Ref	Element	Base	Profile	Support	Notes/References
1	ProbeTransferEnvelope	m	m		
1.1	(per probe fields)				
1.1.1	probe-identifier	m	m		see A.1.5/1
1.1.2	originator-name	m	m		see A.1.7
1.1.3	original-encoded-information-types	m	m-		see A.1.5/3
1.1.4	content-type	m	m-		see A.1.5/8
1.1.5	content-identifier	m	m		
1.1.6	content-length	m	m		
1.1.7	per-message-indicators	m	m		see A.1.5/4
1.1.8	per-domain-bilateral-information	o	m-		see A.1.5/5
1.1.9	trace-information	m	m		see A.1.5/6
1.1.10	extensions				
1.1.10.1	recipient-reassignment-prohibited	o	m		
1.1.10.2	dl-expansion-prohibited	o	m		
1.1.10.3	conversion-with-loss-prohibited	o	m		
1.1.10.4	originator-certificate	o	m-		
1.1.10.5	message-security-label	o	m-		see A.1.6/3
1.1.10.6	content-correlator	m	m		
1.1.10.7	probe-origin-authentication-check	o	m-		see A.1.6/6
1.1.10.8	internal-trace-information	m	m		see A.1.6/5
1.2	per-recipient-fields	m	m		
1.2.1	recipient-name	m	m		see A.1.7
1.2.2	originally-specified-recipient-number	m	m		
1.2.3	per-recipient-indicators	m	m		
1.2.4	explicit-conversion	o	m-		
1.2.5	extensions				

1.2.5.1	originator-requested-alternate-recipient	o	m-		see A.1.7
1.2.5.2	requested-delivery-method	o	m-		
1.2.5.3	physical-rendition-attributes	o	m-		
1.2.5.4	redirection-history	m	m-		

A.1.5 Common data types

Ref	Element	Base	Profile	Support	Notes/References
1	MTSIdentifier				
1.1	global-domain-identifier	m	m		see A.1.5/2
1.2	local-identifier	m	m		
2	GlobalDomainIdentifier				
2.1	country-name	m	m		
2.2	administration-domain-name	m	m		
2.3	private-domain-identifier	m	m		
3	EncodedInformationTypes				
3.1	built-in-encoded-information-types	m	m		
3.2	(non-basic parameters)	o	m-		
3.3	extended-encoded-information-types	m	m		
4	PerMessageIndicators				
4.1	disclosure-of-other-recipients	m	m		
4.2	implicit-conversion-prohibited	m	m		
4.3	alternate-recipient-allowed	m	m		
4.4	content-return-request	o	m-		
4.5	reserved	o	m-		in CCITT X.411 only
4.6	bit-5	o	m-		in CCITT X.411 only
4.7	bit-6	o	m-		in CCITT X.411 only
4.8	service-message	o	m-		in CCITT X.411 only
5	PerDomainBilateralInformation				
5.1	country-name	m	m-		
5.2	administration-domain-name	m	m-		
5.3	private-domain-identifier	o	m-		
5.4	bilateral-information	m	m-		

6	TraceInformation				
6.1	TraceInformationElement	m	m		
6.1.1	global-domain-identifier	m	m		see A.1.5/2
6.1.2	domain-supplied-information	m	m		
6.1.2.1	arrival-time	m	m		
6.1.2.2	routing-action	m	m		
6.1.2.2.1	relayed	m	m		
6.1.2.2.2	rerouted	o	c1		
6.1.2.3	attempted-domain	o	c1		
6.1.2.4	(additional actions)				
6.1.2.4.1	deferred-time	m	c2		
6.1.2.4.2	converted-encoded-information-types	o	m-		see A.1.5/3
6.1.2.4.3	other-actions	o	m-		
6.1.2.4.3.1	redirected	o	m-		
6.1.2.4.3.2	dl-operation	o	m-		
7	LastTraceInformation				
7.1	arrival-time	m	m		
7.2	converted-encoded-information-types	m	m-		see A.1.5/3
7.3	report-type	m	m		
7.3.1	delivery	m	m		
7.3.1.1	message-delivery-time	m	m		
7.3.1.2	type-of-MTS-user	m	m		
7.3.2	non-delivery	m	m		
7.3.2.1	non-delivery-reason-code	m	m		
7.3.2.2	non-delivery-diagnostic-code	m	m		
8	ContentType				
8.1	built-in	m	m-		
8.2	extended	o	m-		

c1 - if rerouting is supported then m else m-c2 - if deferred delivery is supported then m else m-

A.1.6 Extension data types

Ref	Element	Base	Profile	Support	Notes/References
1	ExtensionField				
1.1	type	m	m		
1.1.1	standard-extension	m	m		
1.1.2	private-extension	o	m-		not in CCITT X.411
1.2	criticality	m	m		
1.3	value	m	m		
2	MessageOriginAuthenticationCheck				
2.1	algorithm-identifier	m	m		
2.2	content	m	m		
2.3	content-identifier	o	m		
2.4	message-security-label	o	m		see A.1.6/3
3	MessageSecurityLabel				
3.1	security-policy-identifier	o	m-		
3.2	security-classification	o	m-		
3.3	privacy-mark	o	m-		
3.4	security-categories	o	m-		
4	MessageToken				
4.1	token-type-identifier	m	m		
4.2	asymmetric-token	m	m		
4.2.1	signature-algorithm-identifier	m	m		
4.2.2	name	m	m		
4.2.3	time	m	m		
4.2.4	signed-data	m	m-		
4.2.4.1	content-confidentiality-algorithm-identifier	o	m-		
4.2.4.2	content-integrity-check	o	m-		
4.2.4.3	message-security-label	o	m-		see A.1.6/3

4.2.4.4	proof-of-delivery-request	o	m-		
4.2.4.5	message-sequence-number	o	m-		
4.2.5	encryption-algorithm-identifier	o	m-		
4.2.6	encrypted-data	o	m-		
4.2.6.1	content-confidentiality-key	o	m-		
4.2.6.2	content-integrity-check	o	m-		
4.2.6.3	message-security-label	o	m-		see A.1.6/3
4.2.6.4	content-integrity-key	o	m-		
4.2.6.5	message-sequence-number	o	m-		
5	InternalTraceInformation				
5.1	global-domain-identifier	m	m		
5.2	mta-name	m	m		
5.3	mta-supplied-information	m	m		
5.3.1	arrival-time	m	m		
5.3.2	routing-action	m	m		
5.3.2.1	relayed	m	m		
5.3.2.2	rerouted	o	c1		
5.3.3	attempted	o	c1		
5.3.3.1	mta	o	m		
5.3.3.2	domain	o	m		
5.3.4	(additional actions)				
5.3.4.1	deferred-time	m	c2		
5.3.4.2	converted-encoded-information-types	o	m-		see A.1.5/3
5.3.4.3	other-actions	o	m-		
5.3.4.3.1	redirected	o	m-		
5.3.4.3.2	dl-operation	o	m-		
6	ProbeOriginAuthenticationCheck				
6.1	algorithm-identifier	m	m		

6.2	content-identifier	o	m		
6.3	message-security-label	o	m		see A.1.6/3
7	ProofOfDelivery				
7.1	algorithm-identifier	m	m		
7.2	delivery-time	m	m		
7.3	this-recipient-name	m	m		see A.1.7
7.4	originally-intended-recipient-name	o	m		see A.1.7
7.5	content	m	m		
7.6	content-identifier	o	m		
7.7	message-security-label	o	m		see A.1.6/3
8	ReportOriginAuthenticationCheck				
8.1	algorithm-identifier	m	m		
8.2	content-identifier	o	m		
8.3	message-security-label	o	m		see A.1.6/3
8.4	per-recipient	m	m		
8.4.1	actual-recipient-name	m	m		
8.4.2	originally-intended-recipient-name	o	m		
8.4.3	delivery	o	m		
8.4.3.1	message-delivery-time	m	m		
8.4.3.2	type-of-MTS-user	m	m		
8.4.3.3	recipient-certificate	o	m		
8.4.3.4	proof-of-delivery	o	m		
8.4.4	non-delivery	o	m		
8.4.4.1	non-delivery-reason-code	m	m		
8.4.4.2	non-delivery-diagnostic-code	o	m		

c1 - if rerouting is supported then m else m-

c2 - if deferred delivery is supported then m else m-

A.1.7 O/R names

Ref	O/R Name Form	Base	Profile	Support	Notes/References
1	mnemonic O/R address	m	m-		see A.1.7.1
2	numeric O/R address	m	m-		see A.1.7.2
3	terminal O/R address	m	m-		see A.1.7.3
4	formatted postal O/R address	m	m-		see A.1.7.4
5	unformatted postal O/R address	m	m-		see A.1.7.5
6	directory-name	o	m-		

The following tables shall be completed according to the O/R address forms for which support is claimed above.

NOTE - Classification of an attribute as m indicates only that its presence is required for the O/R address form, not that the capability to make routing decisions on that attribute is required (see also A.3.1).

A.1.7.1 Mnemonic O/R address

Ref	Element	Base	Profile	Support	Notes/References
1	built-in-standard-attributes	m	m		
1.1	country-name	m	m		
1.2	administration-domain-name	m	m		
1.3	private-domain-name	o	m-		
1.4	organization-name	o	m-		
1.5	personal-name	o	m-		
1.5.1	surname	m	m		
1.5.2	given-name	o	m-		
1.5.3	initials	o	m-		
1.5.4	generation-qualifier	o	m-		
1.6	organizational-unit-names	o	m-		
2	built-in-domain-defined-attributes	o	m-		
3	extension-attributes	o	m-		
3.1	common-name	o	m-		
3.2	teletex-common-name	o	m-		
3.3	teletex-organization-name	o	m-		
3.4	teletex-personal-name	o	m-		
3.4.1	surname	m	m		
3.4.2	given-name	o	m-		
3.4.3	initials	o	m-		
3.4.4	generation-qualifier	o	m-		
3.5	teletex-organizational-unit-names	o	m-		
3.6	teletex-domain-defined-attributes	o	m-		

A.1.7.2 Numeric O/R address

Ref	Element	Base	Profile	Support	Notes/References
1	built-in-standard-attributes	m	m		

1.1	country-name	m	m		
1.2	administration-domain-name	m	m		
1.3	private-domain-name	o	m-		
1.4	numeric-user-identifier	m	m		
2	built-in-domain-defined-attributes	o	m-		
3	extension-attributes	o	m-		
3.1	teletex-domain-defined-attributes	o	m-		

A.1.7.3 Terminal O/R address

Ref	Element	Base	Profile	Support	Notes/References
1	built-in-standard-attributes	m	m		
1.1	country-name	o	m-		
1.2	administration-domain-name	o	m-		
1.3	network-address	m	m		
1.4	terminal-identifier	o	m-		
1.5	private-domain-name	o	m-		
2	built-in-domain-defined-attributes	o	m-		
3	extension-attributes	o	m-		
3.1	extended-network-address	m	m		
3.1.1	e163-4-address	o	m-		
3.1.2	psap-address	o	m-		
3.2	terminal-type	o	m-		
3.3	teletex-domain-defined-attributes	o	m-		

A.1.7.4 Formatted postal O/R address

Ref	Element	Base	Profile	Support	Notes/References
1	built-in-standard-attributes	m	m		
1.1	country-name	m	m		
1.2	administration-domain-name	m	m		
1.3	private-domain-name	o	m-		
2	extension-attributes	m	m		
2.1	physical-delivery-country-name	m	m		
2.2	physical-delivery-office-name	o	m-		
2.3	physical-delivery-office-number	o	m-		
2.4	physical-delivery-organization-name	o	m-		
2.5	physical-delivery-personal-name	o	m-		

2.6	postal-code	m	m		
2.7	poste-restante-address	o	m-		
2.8	post-office-box-address	o	m-		
2.9	pds-name	o	m-		
2.10	street-address	o	m-		
2.11	unique-postal-name	o	m-		
2.12	extension-OR-address-components	o	m-		
2.13	extension-physical-delivery-address-components	o	m-		
2.14	local-postal-attributes	o	m-		

A.1.7.5 Unformatted postal O/R address

Ref	Element	Base	Profile	Support	Notes/References
1	built-in-standard-attributes	m	m		
1.1	country-name	m	m		
1.2	administration-domain-name	m	m		
1.3	private-domain-name	o	m-		
2	extension-attributes	m	m		
2.1	unformatted-postal-address	m	m		
2.2	physical-delivery-country-name	m	m		
2.3	postal-code	m	m		
2.4	pds-name	o	m-		

A.2 Optional functional groups

The following requirements are additional to those specified in A.1 if support of the functional group is claimed.

A.2.1 Security (SEC)

The support requirements for all SEC security classes are as specified in A.1 unless otherwise specified below. There are no additional requirements for the confidential security class variants (SnC) above those for the primary security classes.

A.2.1.1 Operation arguments/results

A.2.1.1.1 MTA-bind

Ref	Element	Profile		
		S0	S1	S2
1.2.2	initiator-credentials	mr	mr	mr
1.2.2.1	simple		ix	ix
1.2.2.2	strong		mr	mr
1.2.2.2.1.4	signed-data		mr	mr
1.2.3	security-context		mr	mr
2.2.2	responder-credentials	mr	mr	mr
2.2.2.1	simple		ix	ix
2.2.2.2	strong		mr	mr
2.2.2.2.1.4	signed-data		mr	mr

A.2.1.1.2 Message PDU parameters

Ref	Element	Profile		
		S0	S1	S2
1.1.11.8	message-origin-authentication-check			mr
1.1.11.9	message-security-label		mr	mr
1.2.5.10	message-token		mr	mr
1.2.5.11	content-integrity-check	m	m	m
1.2.5.12	proof-of-delivery-request	m	m	m

A.2.1.1.3 Report PDU parameters

Ref	Element	Profile		
		S0	S1	S2
1.4.1	message-security-label		mr	mr
1.4.5	report-origin-authentication-check			mr

2.2.7.4	proof-of-delivery	m	m	m

A.2.1.1.4 Probe PDU parameters

Ref	Element	Profile		
		S0	S1	S2
1.1.10.5	message-security-label		mr	mr
1.1.10.7	probe-origin-authentication-check			mr

A.2.1.2 Extension data types

Ref	Element	Profile		
		S0	S1	S2
2	MessageOriginAuthenticationCheck			
2.4	message-security-label		mr	mr
3	MessageSecurityLabel			
3.1	security-policy-identifier		mr	mr
3.2	security-classification		m	m
3.4	security-categories		m	m
4	MessageToken			
4.2.4	signed-data	m	m	m
4.2.4.3	message-security-label	m	m	m
4.2.4.4	proof-of-delivery-request	m	m	m
4.2.5	encryption-algorithm-identifier		m	m
4.2.6	encrypted-data		m	m
4.2.6.3	message-security-label	m	m	m
6	ProbeOriginAuthenticationCheck			
6.3	message-security-label		mr	mr
7	ProofOfDelivery			
7.7	message-security-label		mr	mr

8	ReportOriginAuthenticationCheck			
8.3	message-security-label		mr	mr

A.2.2 Physical Delivery (PD)

The support requirements specified below are for an MTA with a co-located PDAU. Support of the PD FG on submission is specified in ISO/IEC ISP 10611-4.

A.2.2.1 Operation arguments/results

A.2.2.1.1 Message PDU parameters

Ref	Element	Profile
1.2.5.5	physical-delivery-modes	m
1.2.5.8	physical-rendition-attributes	m
1.2.5.9	physical-delivery-report-request	m

A.2.2.1.2 Report PDU parameters

Ref	Element	Profile
2.2.7.2	physical-forwarding-address	m

A.2.2.1.3 Probe PDU parameters

Ref	Element	Profile
1.2.5.3	physical-rendition-attributes	m

A.2.2.2 O/R names

Ref	O/R Address Form	Profile
4	formatted postal O/R address	m
5	unformatted postal O/R address	m

A.2.2.2.1 Formatted postal O/R address

Ref	Element	Profile
2.2	physical-delivery-office-name	m
2.3	physical-delivery-office-number	m
2.4	physical-delivery-organization-name	m
2.5	physical-delivery-personal-name	m
2.7	poste-restante-address	m
2.8	post-office-box-address	m
2.9	pds-name	m

2.10	street-address	m
2.11	unique-postal-name	m
2.12	extension-OR-address-components	m
2.13	extension-physical-delivery-address-components	m
2.14	local-postal-attributes	m

A.2.2.2.2 Unformatted postal O/R address

Ref	Element	Profile
2.4	pds-name	m

A.2.3 Conversion (CV)

A.2.3.1 Operation arguments/results

A.2.3.1.1 Message PDU parameters

Ref	Element	Profile
1.1.3	original-encoded-information-types	m
1.1.4	content-type	m
1.2.4	explicit-conversion	c1

c1 - if implicit conversion is not supported then m else o

A.2.3.1.2 Probe PDU parameters

Ref	Element	Profile
1.1.3	original-encoded-information-types	m
1.1.4	content-type	m
1.2.4	explicit-conversion	c1

c1 - if implicit conversion is not supported then m else o

A.2.3.2 Common data types

Ref	Element	Profile
6	TraceInformation	
6.1.2.4.2	converted-encoded-information-types	m
7	LastTraceInformation	
7.2	converted-encoded-information-types	m

A.2.3.3 Extension data types

Ref	Element	Profile
5	InternalTraceInformation	
5.3.4.2	converted-encoded-information-types	m

A.2.4 Redirection (RED)

A.2.4.1 Operation arguments/results

A.2.4.1.1 Message PDU parameters

Ref	Element	Profile
1.2.5.1	originator-requested-alternate-recipient	m
1.2.5.13	redirection-history	m

A.2.4.1.2 Probe PDU parameters

Ref	Element	Profile
1.2.5.1	originator-requested-alternate-recipient	m
1.2.5.4	redirection-history	m

A.2.4.2 Common data types

Ref	Element	Profile
6	TraceInformation	
6.1.2.4.3	other-actions	m
6.1.2.4.3.1	redirected	m

A.2.4.3 Extension data types

Ref	Element	Profile
5	InternalTraceInformation	
5.3.4.3	other-actions	m
5.3.4.3.1	redirected	m

A.2.5 Latest Delivery (LD)

A.2.5.1 Operation arguments/results

A.2.5.1.1 Message PDU parameters

Ref	Element	Profile
1.1.11.4	latest-delivery-time	m

A.2.6 Return of Contents (RoC)

A.2.6.1 Operation arguments/results

A.2.6.1.1 Report PDU parameters

Ref	Element	Profile
2.1.6	returned-content	m

A.2.6.2 Common data types

Ref	Element	Profile
4	PerMessageIndicators	
4.4	content-return-request	m

A.2.7 Distribution List (DL)

A.2.7.1 Operation arguments/results

A.2.7.1.1 Message PDU parameters

Ref	Element	Profile
1.1.11.11	dl-expansion-history	m

A.2.7.1.2 Report PDU parameters

Ref	Element	Profile
1.4.3	reporting-dl-name	m

A.2.7.1.3 Probe PDU parameters

Ref	Element	Profile
1.1.10.8	dl-expansion-history	m

A.2.7.2 Common data types

Ref	Element	Profile
6	TraceInformation	
6.1.2.4.3	other-actions	m
6.1.2.4.3.2	dl-operation	m

A.2.7.3 Extension data types

Ref	Element	Profile
5	InternalTraceInformation	
5.3.4.3	other-actions	m
5.3.4.3.2	dl-operation	m

A.2.8 Use of Directory (DIR)

A.2.8.1 O/R names

Ref	O/R Name Form	Profile
6	directory-name	m

A.3 Additional information

A.3.1 Routing capability

The following table shall be completed to indicate (Y or 3) which O/R address attributes the implementation can use for onward route determination (see clause 8.3 of ISO/IEC ISP 10611-1). Any constraints on the use of an attribute for routing purposes (e.g., whether routing can be based on specific values of the attribute or only on the presence of such attribute, any limitation on the range of values, character repertoires, etc.) shall be indicated in the Comments column.

Ref	O/R Address Attribute	Routable	Comments
1	country-name		
2	administration-domain-name		
3	network-address extended-network-address		
4	terminal-identifier		
5	terminal-type		
6	private-domain-name		
7	organization-name teletex-organization-name		
8	numeric-user-identifier		
9	personal name teletex-personal-name		
10	organizational-unit-names teletex-organizational-unit-names		
11	common-name teletex-common-name		
12	built-in-domain-defined-attributes teletex-domain-defined-attributes		
13	pds-name		
14	physical-delivery-country-name		
15	postal-code		

Any other criteria that can be used to determine routing decisions should be indicated below.

A.3.2 Content types supported

The following table shall be completed to indicate (Y or 3) which content type(s) the implementation can support on transfer (see clause 6 of ISO/IEC ISP 10611-1).

Ref	Content Type	Supported	Comments
1	built-in		
1.1	unidentified (0)		
1.2	external (1)		
1.3	interpersonal-messaging-1984 (2)		
1.4	interpersonal-messaging-1988 (22)		
1.5	(EDI messaging) (35)		

2	extended (specify)		

A.3.3 Encoded information type conversions supported

The following table shall be completed if support of the Conversion FG is claimed, to indicate (Y or 3) which encoded information type conversions the implementation can perform (see clause 7.1 of ISO/IEC ISP 10611-1). The supplier shall also state in the Comments column for which content types support of the conversion capability is claimed and under what conditions loss of information is determined (if applicable).

Ref	Encoded Information Type Conversion	Supported	Comments
1	explicit-conversion		
1.1	ia5-text-to-teletex (0)		
1.2	ia5-text-to-g3-facsimile (8)		
1.3	ia5-text-to-g4-class-1 (9)		
1.4	ia5-text-to-videotex (10)		
1.5	teletex-to-ia5-text (11)		
1.6	teletex-to-g3-facsimile (12)		
1.7	teletex-to-g4-class-1 (13)		
1.8	teletex-to-videotex (14)		
1.9	videotex-to-ia5-text (16)		
1.10	videotex-to-teletex (17)		
2	implicit conversion (specify)		

Annex B

(normative)

Amendments and corrigenda

International Standards are subject to constant review and revision by the ISO/IEC Technical Committees concerned. The following amendments and corrigenda are approved by ISO/IEC JTC1 and are considered as normative references in this part of ISO/IEC ISP 10611.

NOTE - Corresponding corrigenda to the equivalent CCITT Recommendations are contained in the joint CCITT/ISO MHS Implementor's Guide (version 8).

MOTIS

ISO/IEC 10021-1/Cor.1:1991

ISO/IEC 10021-1/Cor.2:1991

ISO/IEC 10021-1/Cor.3:1992

ISO/IEC 10021-1/Cor.4:1992

ISO/IEC 10021-1/Cor.5:1992

ISO/IEC 10021-2/Cor.1:1991

ISO/IEC 10021-2/Cor.2:1991

ISO/IEC 10021-2/Cor.3:1992

ISO/IEC 10021-2/Cor.4:1992

ISO/IEC 10021-4/Cor.1:1991

ISO/IEC 10021-4/Cor.2:1991

ISO/IEC 10021-4/Cor.3:1992

ISO/IEC 10021-4/Cor.4:1992

ISO/IEC 10021-4/Cor.5:1992

ISO/IEC 10021-6/Cor.1:1991

ISO/IEC 10021-6/Cor.2:1991

ISO/IEC 10021-6/Cor.3:1992

ISO/IEC 10021-6/Cor.4:1992

ISO/IEC 10021-6/Cor.5:1992

TITLE: Information technology - International Standardized Profiles AMH1n -
Message Handling Systems - Common Messaging -
Part 4 : AMH12 - MTS Access (P3)

SOURCE: Project Editor (Jon Stranger, UK)

STATUS: DISP text, 1993-7-31

This document forms part of a proposed multipart ISP for MHS covering Common Messaging requirements (AMH1), as identified in the Taxonomy for International Standardized Profiles (ISO/IEC TR 10000-2 : 1992).

This revised DISP version reflects resolution of all remaining outstanding issues at the 6th MHS ISP Special Group (MISG) meeting (Kyoto, February 1-4, 1993) together with some editorial and minor errata which have been determined since submission to ISO/IEC JTC1/SGFS. The content of this document is considered by the MHS expert groups of the three regional workshops as harmonized.

The technical content of this document has been derived wherever possible from the existing EWOS/ETSI and OIW regional profiles in this area. However, differences between the content of this document and one or more regional profiles may exist.

Contents

Annexes

ISO/IEC Copyright Office _ Case Postale 56 _ CH-1211 Genève 20 _ Switzerland

Printed in Switzerland

Foreword

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

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC1. In addition to developing International Standards, ISO/IEC JTC1 has created a Special Group on Functional Standardization for the elaboration of International Standardized Profiles.

An International Standardized Profile is an internationally agreed, harmonized document which identifies a standard or group of standards, together with options and parameters, necessary to accomplish a function or set of functions.

Draft International Standardized Profiles are circulated to national bodies for voting. Publication as an International Standardized Profile requires approval by at least 75% of the national bodies casting a vote.

International Standardized Profile ISO/IEC ISP 10611-4 was prepared with the collaboration of:

- Asia-Oceania Workshop (AOW)

- European Workshop for Open Systems (EWOS) [jointly with the European Telecommunications Standards Institute (ETSI)]

- OSE Implementors' Workshop (OIW)

ISO/IEC ISP 10611 consists of the following parts, under the general title *Information technology - International Standardized Profiles AMH1n - Message Handling Systems - Common Messaging*:

- Part 1 : MHS Service Support

- Part 2 : Specification of ROSE, RTSE, ACSE, Presentation and Session

Protocols for use by MHS

- Part 3 : AMH11 - Message Transfer (P1)

- Part 4 : AMH12 - MTS Access (P3)

- Part 5 : AMH13 - MS Access (P7)

This part of ISO/IEC ISP 10611 contains two annexes, A and B, which are normative.

Introduction

This part of International Standardized Profile ISO/IEC ISP 10611 is defined within the context of Functional Standardization, in accordance with the principles specified by ISO/IEC TR 10000, “Framework and Taxonomy of International Standardized Profiles”. The context of Functional Standardization is one part of the overall field of Information Technology (IT) standardization activities, covering base standards, profiles, and registration mechanisms. A profile defines a combination of base standards that collectively perform a specific well-defined IT function. Profiles standardize the use of options and other variations in the base standards, and provide a basis for the development of uniform, internationally recognized system tests.

One of the most important rôles for an ISP is to serve as the basis for the development (by organizations other than ISO and IEC) of internationally recognized tests and test centres. ISPs are produced not simply to ‘legitimize' a particular choice of base standards and options, but to promote real system interoperability. The development and widespread acceptance of tests based on this and other ISPs is crucial to the successful realization of this goal.

The text for this part of ISO/IEC ISP 10611 was developed in close cooperation between the MHS Expert Groups of the three Regional Workshops: the North American OSE Implementors' Workshop (OIW), the European Workshop for Open Systems (EWOS) (jointly with the corresponding expert group of the European Telecommunications Standards Institute - ETSI) and the OSI Asia-Oceania Workshop (AOW). This part of ISO/IEC ISP 10611 is harmonized between these three Workshops and it has been ratified by the plenary assemblies of all three Workshops.

Information technology - International Standardized Profiles AMH1n - Message Handling Systems - Common Messaging

Part 4 : AMH12 - MTS Access (P3)

1 Scope

1.1 General

This part of ISO/IEC ISP 10611 covers access to a Message Transfer System (MTS) using the P3 MTS Access Protocol (see also figure 1). These specifications form part of the Common Messaging application functions, as defined in the parts of ISO/IEC ISP 10611, which form a common basis for content type-dependent International Standardized Profiles for MHS that will be developed.

1.2 Position within the taxonomy

This part of ISO/IEC ISP 10611 is the fourth part of a multipart ISP identified in ISO/IEC TR 10000-2 as “AMH1, Message Handling Systems - Common Messaging” (see also ISO/IEC TR 10000-1, 8.2 for the definition of multipart ISPs).

This part of ISO/IEC ISP 10611 specifies the following profile:

AMH12 - MTS Access (P3)

The AMH12 profile may be combined with any T-Profiles (see ISO/IEC TR 10000) specifying the OSI connection-mode Transport service.

1.3 Scenario

The model used is one of access to an MTS by an MTS-user - specifically, the intercommunication between a message transfer agent (MTA) and an MTS-user using the P3 protocol, as shown in figure 1.

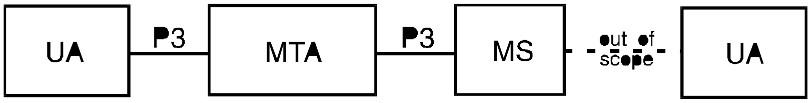


Figure 1 - AMH12 scenario

The AMH12 profile covers all aspects of the MTS Abstract Service, as defined in clause 8 of ISO/IEC 10021-4, when realized using the P3 protocol.

The OSI upper layer services and protocols to support the Message Handling Systems functions covered by the AMH12 profile are specified in the set of standards identified in table 1.

Table 1 - AMH12 profile model

Application Layer	MHS	ISO/IEC 10021-6
	ROSE	see ISO/IEC ISP 10611-2
	RTSE	see ISO/IEC ISP 10611-2
	ACSE	see ISO/IEC ISP 10611-2
Presentation Layer		see ISO/IEC ISP 10611-2
Session Layer		see ISO/IEC ISP 10611-2

2 Normative references

The following documents contain provisions which, through reference in this text, constitute provisions of this part of ISO/IEC ISP 10611. At the time of publication, the editions indicated were valid. All documents are subject to revision, and parties to agreements based on this part of ISO/IEC ISP 10611 are warned against automatically applying any more recent editions of the documents listed below, since the nature of references made by ISPs to such documents is that they may be specific to a particular edition. Members of IEC and ISO maintain registers of currently valid International Standards and ISPs, and CCITT maintains published editions of its current Recommendations.

Amendments and corrigenda to the base standards referenced are listed in annex B.

NOTE - References in the body of this part of ISO/IEC ISP 10611 to specific clauses of ISO/IEC documents shall be considered to refer also to the corresponding clauses of the equivalent CCITT Recommendations (as noted below) unless otherwise stated.

ISO/IEC TR 10000-1: 1992, *Information technology - Framework and taxonomy of International Standardized Profiles - Part 1: Framework.*

ISO/IEC TR 10000-2: 1992, *Information technology - Framework and taxonomy of International Standardized Profiles - Part 2: Taxonomy.*

ISO/IEC 10021-1: 1990, *Information technology - Text Communication - Message-Oriented Text Interchange Systems (MOTIS) - Part 1: Service Overview. [see also CCITT Recommendation X.400(1988)]*

ISO/IEC 10021-2: 1990, *Information technology - Text Communication - Message-Oriented Text Interchange Systems (MOTIS) - Part 2: Overall Architecture. [see also CCITT Recommendation X.402(1988)]*

ISO/IEC 10021-4: 1990, *Information technology - Text Communication - Message-Oriented Text Interchange Systems (MOTIS) - Part 4: Message Transfer System: Abstract Service Definition and Procedures. [see also CCITT Recommendation X.411(1988)]*

ISO/IEC 10021-6: 1990, *Information technology - Text Communication - Message-Oriented Text Interchange Systems (MOTIS) - Part 6: Protocol Specifications. [see also CCITT Recommendation X.419(1988)]*

ISO/IEC ISP 10611-1: ---[2], *Information technology - International Standardized Profiles AMH1n - Message Handling Systems - Common Messaging - Part 1: MHS Service Support.*

ISO/IEC ISP 10611-2: ---[1], *Information technology - International Standardized Profiles AMH1n - Message Handling Systems - Common Messaging - Part 2: Specification of ROSE, RTSE, ACSE, Presentation and Session Protocols for use by MHS.*

CCITT Recommendation X.400(1988), *Message handling system and service overview.*

CCITT Recommendation X.402(1988), *Message handling systems: Overall architecture.*

[2] To be published.

CCITT Recommendation X.411(1988)*, Message handling systems: Message transfer system: Abstract service definition and procedures.*

CCITT Recommendation X.419(1988)*, Message handling systems: Protocol specifications.*

MHS Implementors' Guide, Version 8, March 1992 (CCITT Special Rapporteur's Group on Message Handling Systems and ISO/IEC JTC1/SC18/WG4 SWG on Messaging).

3 Definitions

For the purposes of this part of ISO/IEC ISP 10611, the following definitions apply.

Terms used in this part of ISO/IEC ISP 10611 are defined in the referenced base standards; in addition, the following terms are defined.

3.1 General

Basic requirement : an Element of Service, protocol element, procedural element or other identifiable feature specified in the base standards which is required to be supported by all MHS implementations.

Functional group : a specification of one or more related Elements of Service, protocol elements, procedural elements or other identifiable features specified in the base standards which together support a significant optional area of MHS functionality.

NOTE - A functional group can cover any combination of MHS features specified in the base standards for which the effect of implementation can be determined at a standardized external interface - i.e., via a standard OSI communications protocol (other forms of exposed interface, such as a standardized programmatic interface, are outside the scope of this version of ISO/IEC ISP 10611).

3.2 Support classification

To specify the support level of operations, arguments, results and other protocol features for this part of ISO/IEC ISP 10611, the following terminology is defined.

3.2.1 Static capability

The following classifications are used in this part of ISO/IEC ISP 10611 to specify static conformance requirements - i.e., capability.

In the case of arguments and results (protocol elements), the classification is relative to that of the containing element, if any. Where the constituent elements of a non-primitive element are not individually specified, then each shall be considered to have the classification of that element. Where the range of values to be supported for an element is not specified, then all values defined in the MHS base standards shall be supported.

mandatory full support (**m**) : the element or feature shall be fully supported. An implementation shall be able to generate the element, and/or receive the element and perform all associated procedures (i.e., implying the ability to handle both the syntax and the semantics of the element) as relevant, as specified in the MHS base standards. Where support for origination (generation) and reception are not distinguished, then both capabilities shall be assumed.

mandatory minimal support (**m-**) : the element shall be supported. However, an implementation is only required to be able to copy the syntax of the element to the corresponding element of a message, probe or report for onward transfer or delivery, as appropriate, according to the procedures as specified in the MHS base standards, unless further qualified for the output envelope in question elsewhere in this ISP (i.e., the classification of the output envelope takes precedence). An implementation is not required to be able to take any explicit action based on the semantics of such an element other than to obey criticality. An implementation is not required to be able to originate such an element.

NOTE - The m- classification is designed to distinguish those cases where the MHS base standards define more than one level of functionality and the minimum required level of support in this profile is the minimum functionality defined in the base standards. Where the only functionality defined in the base standards is copying the element as described above, then the m classification is used in preference to m-.

optional support (**o**) : an implementation is not required to support the element or feature. If support is claimed, the element shall be treated as if it were specified as mandatory support. If support for origination is not claimed, then the element is not generated and, in the case of non-support of a critical extension by an MTA implementation on delivery, shall cause a non-delivery notification to be returned. If support for reception is not claimed, and the element is an argument, then an implementation may ignore a non-critical extension on delivery but shall otherwise generate an appropriate error. If support for reception is not claimed, and the element is a result, then the element may be ignored.

conditional support (**c**) : the element shall be supported under the conditions specified in this part of ISO/IEC ISP 10611. If these conditions are met, the element shall be treated as if it were specified as mandatory support. If these conditions are not met, the element shall be treated as if it were specified as optional support (unless otherwise stated).

out of scope (**i**) : the element is outside the scope of this part of ISO/IEC ISP 10611 - i.e., it will not be the subject of an ISP conformance test.

not applicable (**–**) : the element is not applicable in the particular context in which this classification is used.

3.2.2 Dynamic behaviour

The above classifications are used in this part of ISO/IEC ISP 10611 to specify static conformance requirements (i.e., capability); dynamic conformance requirements (i.e., behaviour) are as specified in the MHS base standards. However, in a few cases it has been necessary to specify additional dynamic conformance requirements in this profile. These are specified using a second classification code for an element, as follows.

NOTE - Clause 6.7 of ISO/IEC TR 10000-1 states that a profile shall not introduce a constraint on dynamic behaviour on reception. However, in the case of MHS security (at least), the base standards define a suitable error indication to cover the breach of a security policy but do not specify the precise conditions under which such error indication shall be used. Any such specification in a profile is thus a legitimate qualification of the base standards rather than a modification of such provisions.

required (**r**) : the element shall always be present. An implementation shall ensure that the element is always generated or otherwise used, as appropriate. Absence of the element on reception shall result in termination or rejection of the communication with an appropriate error indication as specified in the MHS base standards.

excluded (**x**) : the element shall never be present. An implementation shall ensure that the element is never generated or otherwise used, as appropriate. Presence of the element on reception shall result in termination or rejection of the communication with an appropriate error indication as specified in the MHS base standards.

NOTE - It is recognized that some implementations may be required to exclude even a static capability in such cases, but such considerations are outside the scope of this profile. Any elements which are specified as excluded (x) in this profile are thus also specified as out of scope (i) in terms of static capability.

4 Abbreviations

AMH	Application Message Handling
ASN.1	Abstract Syntax Notation One
CV	Conversion
DIR	Use of Directory
DL	Distribution List
EoS	Element of Service
FG	Functional group
ISP	International Standardized Profile
LD	Latest Delivery
MHS	Message Handling Systems
MS	Message store
MTA	Message transfer agent
OSI	Open Systems Interconnection
PD	Physical Delivery
RED	Redirection
RoC	Return of Contents
SEC	Security
UA	User agent

Support level for protocol elements and features (see 3.2):

m	mandatory full support
m-	mandatory minimal support
o	optional support
c	conditional support
i	out of scope
–	not applicable
r	required
x	excluded

5 Conformance

This part of ISO/IEC ISP 10611 states requirements upon implementations to achieve interworking. A claim of conformance to this part of ISO/IEC ISP 10611 is a claim that all requirements in the relevant base standards are satisfied, and that all requirements in the following clauses and in annex A of this part of ISO/IEC ISP 10611 are satisfied. Annex A states the relationship between these requirements and those of the base standards.

5.1 Conformance statement

For each implementation claiming conformance to profile AMH12 as specified in this part of ISO/IEC ISP 10611, a PICS shall be made available stating support or non-support of each option identified in this part of ISO/IEC ISP 10611.

The scope of conformance to profile AMH12 covers both MTAs and MTS-users. A claim of conformance to profile AMH12 shall state whether the implementation claims conformance as an MTA, as a UA, or as an MS which is not co-located with an MTA.

5.2 MHS conformance

This part of ISO/IEC ISP 10611 specifies implementation options or selections such that conformant implementations will satisfy the conformance requirements of ISO/IEC 10021 and the CCITT X.400 Recommendations.

Implementations conforming to profile AMH12 as specified in this part of ISO/IEC ISP 10611 shall implement all the mandatory support (m or m-) features identified as basic requirements in annex A and shall state which optional support (o) features are implemented. They shall also support corresponding MHS Elements of Service and associated procedures as specified in ISO/IEC ISP 10611-1, as appropriate to the scope of this profile and to the role (i.e., MTA or MTS-user) for which conformance is claimed.

Implementations conforming to profile AMH12 as specified in this part of ISO/IEC ISP 10611 shall state whether or not they support any of the optional functional groups as specified in ISO/IEC ISP 10611-1 which are applicable to the scope of this profile and to the role (i.e., MTA or MTS-user) for which conformance is claimed. For each functional group for which support is claimed, an implementation shall implement all the mandatory support (m or m-) features identified for that functional group in annex A and shall state which optional support (o) features are implemented. They shall also support corresponding MHS Elements of Service and associated procedures as specified in ISO/IEC ISP 10611-1, as appropriate to the scope of this profile and to the role (i.e., MTA or MTS-user) for which conformance is claimed.

Implementations conforming to profile AMH12 as specified in this part of ISO/IEC ISP 10611 shall state the P3 application context(s) for which conformance is claimed.

5.3 Underlying layers conformance

Implementations conforming to profile AMH12 as specified in this part of ISO/IEC ISP 10611 shall also conform to ISO/IEC ISP 10611-2 in accordance with the P3 application context(s) for which conformance is claimed.

Annex A[1]

(normative)

ISPICS Proforma

for ISO/IEC ISP 10611-4 (AMH12)

In the event of a discrepancy becoming apparent in the body of this part of ISO/IEC ISP 10611 and the tables in this annex, this annex is to take precedence.

[**Editor's Note** : It had been intended that this annex would eventually be based on the ISO/IEC 10021 P3 PICS proforma. However, the current version of the latter (as contained in ISO/IEC CD 10021-13) is defective and the whole ISO/IEC work item for the development of MOTIS PICS proformas has now been suspended. As a result, it has been necessary to turn the P3 IPRL in this annex into a complete ISPICS (the alternative approach of a separate annex containing the assumed base standard PICS proforma was not considered appropriate in this case). This annex broadly follows the final draft of CCITT Recommendation X.483 (April 1992), but the structure has been modified to some extent to take account of profiling requirements and the somewhat different conformance objectives.]

Clause A.1 specifies the basic requirements for conformance to profile AMH12. Clause A.2 specifies additional requirements to those specified in A.1 for each of the optional functional groups if conformance to such a functional group is claimed. Clause A.3 allows additional information to be provided for certain aspects of an implementation where no specific requirements are included in ISO/IEC ISP 10611. All three clauses shall be completed as appropriate.

In each table, the "Base" column reflects the level of support required for conformance to the base standard and the "Profile" column specifies the level of support required by this ISP (using the classification and notation defined in 3.2).

[**Editor's Note** : The identification of the base standard requirement has in some cases had to be interpreted or varied from that specified in the current CCITT PICS proforma, either due to the different classification scheme employed or where the base standard is unclear and it has been considered that the CCITT PICS proforma is in error.]

The Support column is provided for completion by the supplier of the implementation as follows:

Y	the element or feature is fully supported (i.e., satisfying the requirements of the m profile support classification)
Y-	the element or feature is minimally supported (i.e., satisfying the requirements of the m- profile support classification)
N	the element or feature is not supported, further qualified to indicate the action taken on receipt of such an element as follows:

[1] **Copyright release for ISPICS proformas**
Users of this International Standardized Profile may freely reproduce the ISPICS proforma in this annex so that it can be used for its intended purpose and may further publish the completed ISPICS.

	ND - the element is discarded/ignored NR - the PDU is rejected (with an appropriate error indication where applicable)
– or blank	the element or feature is not applicable (i.e., a major feature or composite protocol element which includes this element or feature is not supported)

Identification of the implementation

Identification of PICS

Ref	Question	Response
1	Date of statement (DD/MM/YY)	
2	PICS serial number	
3	System conformance statement cross reference	

Identification of IUT

Ref	Question	Response
1	Implementation name	
2	Implementation version	
3	Machine name	
4	Machine version	
5	Operating system name	
6	Operating system version	
7	Special configuration	
8	Other information	

Identification of supplier

Ref	Question	Response
1	Organization name	
2	Contact name(s)	
3	Address	
4	Telephone number	
5	Telex number	
6	Fax number	
7	E-mail address	
8	Other information	

Identification of protocol

Ref	Question	Response
1	Title, reference number and date of publication of the protocol standard	
2	Protocol version(s)	
3	Addenda/amendments/corrigenda implemented	
4	Defect reports implemented	

Type of implementation

Ref	Implementation Type	Response
1	MTS-user (UA or MS)	
2	MTA	

NOTE - A separate PICS shall be completed for each implementation type for which conformance is claimed.

Global statement of conformance

Ref	Question	Response
1	Are all mandatory base standards requirements implemented?	

Statement of profile conformance

Ref	Question	Response	Comments
1	Are all mandatory requirements of profile AMH12 implemented?		
2	Are all mandatory requirements of any of the following optional functional groups implemented?		
2.1	Security (SEC)		class(es):
2.2	Physical Delivery (PD)		
2.3	Conversion (CV)		
2.4	Redirection (RED)		
2.5	Latest Delivery (LD)		
2.6	Return of Contents (RoC)		
2.7	Distribution List (DL)		
2.8	Use of Directory (DIR)		

A.1 Basic requirements

A.1.1 Supported application contexts

Ref	Application Context	MTS-user		MTA		Support	Notes/References
		Base	Profile	Base	Profile		
1	mts-access	m	m	m	m		
2	mts-forced-access	m	m	m	m		
3	mts-reliable-access	o	o	o	o		
4	mts-forced-reliable-access	o	o	o	o		

A.1.2 Supported operations

A.1.2.1 Bind and Unbind

Ref	Operation	MTS-user		MTA		Support	Notes/References
		Base	Profile	Base	Profile		
1	MTSBInd access	m	m	m	m		see A.1.3.1
2	MTSUnbind access	m	m	m	m		
3	MTSBind forced access	m	m	m	m		see A.1.3.1
4	MTSUnbind forced access	m	m	m	m		

A.1.2.2 Message Submission Service Element (MSSE)

Ref	Operation	MTS-user		MTA		Support	Notes/References
		Base	Profile	Base	Profile		
1	MessageSubmission	m	m	m	m		see A.1.3.2
2	ProbeSubmission	o	o	m	m		see A.1.3.3
3	CancelDeferredDelivery	o	o	m	m		see A.1.3.4
4	SubmissionControl	m	m	o	o		see A.1.3.5

NOTE - If the MTS-user is an MS, then the requirement is only to be able to pass through these operations (ie, between the MTA and a local or remote UA) unaltered.

A.1.2.3 Message Delivery Service Element (MDSE)

Ref	Operation	MTS-user		MTA		Support	Notes/References
		Base	Profile	Base	Profile		
1	MessageDelivery	m	m	m	m		see A.1.3.6
2	ReportDelivery	m	m	m	m		see A.1.3.7
3	DeliveryControl	o	o	m	m		see A.1.3.8

A.1.2.4 Message Administration Service Element (MASE)

Ref	Operation	MTS-user		MTA		Support	Notes/References
		Base	Profile	Base	Profile		
1	Register	o	o	o	o		see A.1.3.9
2	ChangeCredentials (MTA to UA)	o	o	o	o		see A.1.3.10
3	ChangeCredentials (UA to MTA)	o	o	o	o		see A.1.3.10

NOTE - If the MTS-user is an MS, then the requirement is only to be able to pass through these operations (ie, between the MTA and a local or remote UA) unaltered. For a UA or MTA, some or all of the services and functionality supported by these operations may be implemented by other means as a local matter.

A.1.3 Operation arguments/results

A.1.3.1 MTS-bind

Ref	Element	MTS-user		MTA		Support	Notes/References
		Base	Profile	Base	Profile		
1	ARGUMENT						
1.1	initiator-name	m	m	m	m		
1.2	messages-waiting	o	c1	o	c1		
1.3	initiator-credentials	m	m	m	m		
1.3.1	simple	m	m	m	m		
1.3.1.1	OCTET STRING	o	m	o	m		
1.3.1.2	IA5String	o	o	o	o		
1.3.2	strong	o	o	o	o		
1.3.2.1	bind-token	m	m	m	m		
1.3.2.1.1	signature-algorithm-identifier	m	m	m	m		
1.3.2.1.2	name	m	m	m	m		
1.3.2.1.3	time	m	m	m	m		
1.3.2.1.4	signed-data	o	o	o	o		
1.3.2.1.5	encryption-algorithm-identifier	o	o	o	o		
1.3.2.1.6	encrypted-data	o	o	o	o		
1.3.2.2	certificate	o	o	o	o		
1.4	security-context	o	o	o	o		see A.1.9/3
2	RESULT						
2.1	responder-name	m	m	m	m		
2.2	messages-waiting	o	c2	o	c2		
2.3	responder-credentials	m	m	m	m		
2.3.1	simple	m	m	m	m		
2.3.1.1	OCTET STRING	o	m	o	m		
2.3.1.2	IA5String	o	o	o	o		
2.3.2	strong	o	o	o	o		

2.3.2.1	bind-token	m	m	m	m		
2.3.2.1.1	signature-algorithm-identifier	m	m	m	m		
2.3.2.1.2	name	m	m	m	m		
2.3.2.1.3	time	m	m	m	m		
2.3.2.1.4	signed-data	o	o	o	o		
2.3.2.1.5	encryption-algorithm-identifier	o	o	o	o		
2.3.2.1.6	encrypted-data	o	o	o	o		

c1 - if the MTA is the initiator then m else –

c2 - if the MTS-user is the initiator then m else –

A.1.3.2 MessageSubmission

Ref	Element	UA		MTA		Support	Notes/References
		Base	Profile	Base	Profile		
1	ARGUMENT						
1.1	envelope	m	m	m	m		see A.1.4
1.2	content	m	m	m	m		
2	RESULT						
2.1	message-submission-identifier	m	m	m	m		see A.1.8/1
2.2	message-submission-time	m	m	m	m		
2.3	content-identifier	o	c1	m	m		
2.4	extensions						
2.4.1	originating-MTA-certificate	o	i	o	i		
2.4.2	proof-of-submission	o	i	o	i		see A.1.9/7

c1 - if supported in message submission envelope then m else –

A.1.3.3 ProbeSubmission

Ref	Element	UA		MTA		Support	Notes/References
		Base	Profile	Base	Profile		
1	ARGUMENT						
1.1	envelope	m	m	m	m		see A.1.5
2	RESULT						
2.1	probe-submission-identifier	m	m	m	m		see A.1.8/1
2.2	probe-submission-time	m	m	m	m		
2.3	content-identifier	o	c1	m	m		

c1 - if supported in probe submission envelope then m else –

A.1.3.4 CancelDeferredDelivery

Ref	Element	UA		MTA		Support	Notes/References
		Base	Profile	Base	Profile		
1	ARGUMENT						
1.1	message-submission-identifier	m	m	m	m		see A.1.8/1
2	RESULT						
2.1	NULL	m	m	m	m		

A.1.3.5 SubmissionControl

Ref	Element	UA		MTA		Support	Notes/References
		Base	Profile	Base	Profile		
1	ARGUMENT						
1.1	controls	m	m	m	m		
1.1.1	restrict	m	m	o	m		
1.1.2	permissible-operations	m	m	o	o		
1.1.3	permissible-maximum-content-length	m	m	o	o		
1.1.4	permissible-lowest-priority	m	m	o	o		
1.1.5	permissible-security-context	o	o	o	o		see A.1.9/3
2	RESULT						
2.1	waiting	m	m	m	m		
2.1.1	waiting-operations	o	o	m	m		
2.1.2	waiting-messages	o	o	m	m		
2.1.3	waiting-content-types	o	o	m	m		
2.1.4	waiting-encoded-information-types	o	o	m	m		see A.1.8/3

A.1.3.6 MessageDelivery

Ref	Element	MTS-user		MTA		Support	Notes/References
		Base	Profile	Base	Profile		

1	ARGUMENT						
1.1	(envelope)	m	m	m	m		see A.1.6
1.2	content	m	m	m	m		
2	RESULT						
2.1	recipient-certificate	o	o	o	o		
2.2	proof-of-delivery	o	o	o	o		see A.1.9/6

A.1.3.7 ReportDelivery

Ref	Element	MTS-user		MTA		Support	Notes/References
		Base	Profile	Base	Profile		
1	ARGUMENT						
1.1	(envelope)	m	m	m	m		see A.1.7
1.2	returned-content	o	c1	o	m-		
2	RESULT						
2.1	NULL	m	m	m	m		

c1 - if supported in message submission envelope then m else –

A.1.3.8 DeliveryControl

Ref	Element	MTS-user		MTA		Support	Notes/References
		Base	Profile	Base	Profile		
1	ARGUMENT						
1.1	controls	m	m	m	m		
1.1.1	restrict	m	m	m	m		
1.1.2	permissible-operations	o	o	m	m		
1.1.3	permissible-maximum-content-length	o	o	m	m		
1.1.4	permissible-lowest-priority	o	o	m	m		
1.1.5	permissible-content-types	o	o	m	m		
1.1.6	permissible-encoded-information-types	o	o	m	m		see A.1.8/3
1.1.5	permissible-security-context	o	o	o	o		see A.1.9/3
2	RESULT						
2.1	waiting	m	m	m	m		
2.1.1	waiting-operations	m	m	o	o		
2.1.2	waiting-messages	m	m	o	o		
2.1.3	waiting-content-types	m	m	o	o		
2.1.4	waiting-encoded-information-types	m	m	o	o		see A.1.8/3

A.1.3.9 Register

Ref	Element	UA		MTA		Support	Notes/References
		Base	Profile	Base	Profile		
1	ARGUMENT						
1.1	user-name	o	o	o	o		see A.1.10
1.2	user-address	o	o	o	o		
1.3	deliverable-encoded-information-types	o	o	o	m		see A.1.8/3
1.4	deliverable-maximum-content-length	o	o	o	m		
1.5	default-delivery-controls	o	o	o	o		
1.5.1	restrict	o	o	o	m		
1.5.2	permissible-operations	o	o	o	m		

1.5.3	permissible-maximum-content-length	o	o	o	m		
1.5.4	permissible-lowest-priority	o	o	o	m		
1.5.5	permissible-content-types	o	o	o	m		
1.5.6	permissible-encoded-information-types	o	o	o	m		see A.1.8/3
1.6	deliverable-content-types	o	o	o	m		
1.7	labels-and-redirections	o	o	o	o		
1.7.1	user-security-label	o	o	o	o		see A.1.9/3
1.7.2	recipient-assigned-alternate-recipient	o	o	o	o		
2	RESULT						
2.1	NULL	m	m	m	m		

A.1.3.10 ChangeCredentials

Ref	Element	UA		MTA		Support	Notes/References
		Base	Profile	Base	Profile		
1	ARGUMENT						
1.1	old-credentials	m	m	m	m		
1.1.1	simple	m	m	m	m		
1.1.1.1	OCTET STRING	o	m	o	m		
1.1.1.2	IA5String	o	o	o	o		
1.1.2	strong	o	o	o	o		
1.1.2.1	bind-token	m	m	m	m		see A.1.3.1
1.1.2.2	certificate	o	o	o	o		
1.2	new-credentials	m	m	m	m		
1.2.1	simple	m	m	m	m		
1.2.1.1	OCTET STRING	o	m	o	m		
1.2.1.2	IA5String	o	o	o	o		
1.2.2	strong	o	o	o	o		
1.2.2.1	bind-token	m	m	m	m		see A.1.3.1
1.2.2.2	certificate	o	o	o	o		
2	RESULT						
2.1	NULL	m	m	m	m		

A.1.4 MessageSubmissionEnvelope

Ref	Element	UA		MTA		Support	Notes/References
		Base	Profile	Base	Profile		
1	originator-name	m	m	m	m		see A.1.10
2	original-encoded-information-types	m	m	m	m-		see A.1.8/3
3	content-type	m	m	m	m-		
4	content-identifier	o	o	m	m		

5	priority	m	m	m	m		
6	per-message-indicators	m	m	m	m		see A.1.8/5
7	deferred-delivery-time	o	o	m	m		
8	extensions						
8.1	recipient-reassignment-prohibited	o	m1	o	m		
8.2	dl-expansion-prohibited	o	m1	o	m		
8.3	conversion-with-loss-prohibited	o	o	o	m		
8.4	latest-delivery-time	o	o	o	o		
8.5	originator-return-address	o	o	o	o		see A.1.10
8.6	originator-certificate	o	o	o	o		
8.7	content-confidentiality-algorithm-identifier	o	o	o	o		
8.8	message-origin-authentication-check	o	o	o	o		see A.1.9/2
8.9	message-security-label	o	o	o	o		see A.1.9/3
8.10	proof-of-submission-request	o	i	o	i		
8.11	content-correlator	o	o	m	m		
9	per-recipient-fields	m	m	m	m		
9.1	recipient-name	m	m	m	m		see A.1.10
9.2	originator-report-request	m	m	m	m		
9.3	explicit-conversion	o	o	o	m-		
9.4	extensions						
9.4.1	originator-requested-alternate-recipient	o	o	o	o		see A.1.10
9.4.2	requested-delivery-method	o	o	o	o		
9.4.3	physical-forwarding-prohibited	o	o	o	o		
9.4.4	physical-forwarding-address-request	o	o	o	o		
9.4.5	physical-delivery-modes	o	o	o	o		
9.4.6	registered-mail-type	o	o	o	o		
9.4.7	recipient-number-for-advice	o	o	o	o		
9.4.8	physical-rendition-attributes	o	o	o	o		
9.4.9	physical-delivery-report-request	o	o	o	o		

9.4.10	message-token	o	o	o	o		see A.1.9/4
9.4.11	content-integrity-check	o	o	o	o		
9.4.12	proof-of-delivery-request	o	o	o	o		

m1 - only the capability to generate the "prohibited" value is required

A.1.5 ProbeSubmissionEnvelope

Ref	**Element**	**UA**		**MTA**		**Support**	**Notes/References**
		Base	**Profile**	**Base**	**Profile**		
1	originator-name	m	m	m	m		see A.1.10
2	original-encoded-information-types	m	m	m	m-		see A.1.8/3
3	content-type	m	m	m	m-		
4	content-identifier	o	o	m	m		
5	content-length	o	m	m	m		
6	per-message-indicators	m	m	m	m		see A.1.8/5
7	extensions						
7.1	recipient-reassignment-prohibited	o	m1	o	m		
7.2	dl-expansion-prohibited	o	m1	o	m		
7.3	conversion-with-loss-prohibited	o	o	o	m		
7.4	originator-certificate	o	o	o	o		
7.5	message-security-label	o	o	o	o		see A.1.9/3
7.6	content-correlator	o	o	m	m		
7.7	probe-origin-authentication-check	o	o	o	o		see A.1.9/5
8	per-recipient-fields	m	m	m	m		
8.1	recipient-name	m	m	m	m		see A.1.10
8.2	originator-report-request	m	m	m	m		
8.3	explicit-conversion	o	o	o	m-		
8.4	extensions						
8.4.1	originator-requested-alternate-recipient	o	o	o	o		see A.1.10
8.4.2	requested-delivery-method	o	o	o	o		

8.4.3	physical-rendition-attributes	o	o	o	o		

m1 - only the capability to generate the "prohibited" value is required

A.1.6 MessageDeliveryEnvelope

Ref	Element	MTS-user		MTA		Support	Notes/References
		Base	Profile	Base	Profile		
1	message-delivery-identifier	m	m	m	m		see A.1.8/1
2	message-delivery-time	m	m	m	m		
3	other-fields	m	m	m	m		
3.1	content-type	m	m	m	m		
3.2	originator-name	m	m	m	m		see A.1.10
3.3	original-encoded-information-types	m	m	m	m		see A.1.8/3
3.4	priority	m	m	m	m		
3.5	delivery-flags	m	m	m	m		
3.5.1	implicit-conversion-prohibited	m	m	m	m		
3.6	other-recipient-names	m	m	m	m		see A.1.10
3.7	this-recipient-name	m	m	m	m		see A.1.10
3.8	originally-intended-recipient-name	m	m	m	m		see A.1.10
3.9	converted-encoded-information-types	m	m	m	m		see A.1.8/3
3.10	message-submission-time	m	m	m	m		
3.11	content-identifier	o	m	m	m		
3.12	extensions						
3.12.1	conversion-with-loss-prohibited	o	o	o	m		
3.12.2	requested-delivery-method	o	o	o	o		
3.12.3	physical-forwarding-prohibited	o	o	o	o		
3.12.4	physical-forwarding-address-request	o	o	o	o		
3.12.5	physical-delivery-modes	o	o	o	o		
3.12.6	registered-mail-type	o	o	o	o		
3.12.7	recipient-number-for-advice	o	o	o	o		
3.12.8	physical-rendition-attributes	o	o	o	o		
3.12.9	originator-return-address	o	o	o	o		
3.12.10	physical-delivery-report-request	o	o	o	o		

3.12.11	originator-certificate	o	o	o	o		
3.12.12	message-token	o	o	o	o		see A.1.9/4
3.12.13	content-confidentiality-algorithm-identifier	o	o	o	o		
3.12.14	content-integrity-check	o	o	o	o		
3.12.15	message-origin-authentication-check	o	o	o	o		see A.1.9/2
3.12.16	message-security-label	o	o	o	o		see A.1.9/3
3.12.17	proof-of-delivery-request	o	o	o	o		
3.12.18	redirection-history	o	o	m	m		
3.12.19	dl-expansion-history	o	o	m	m		

A.1.7 ReportDeliveryEnvelope

Ref	Element	MTS-user		MTA		Support	Notes/References
		Base	Profile	Base	Profile		
1	subject-submission-identifier	m	m	m	m		see A.1.8/1
2	content-identifier	o	c1	m	m		
3	content-type	m	m	m	m		
4	original-encoded-information-types	m	m	m	m		see A.1.8/3
5	extensions						
5.1	message-security-label	o	c1	o	o		see A.1.9/3
5.2	content-correlator	o	c1	m	m		
5.3	originator-and-DL-expansion-history	m	m	m	m		
5.4	reporting-DL-name	o	m	o	m		see A.1.10
5.5	reporting-MTA-certificate	o	o	o	o		
5.6	report-origin-authentication-check	o	o	o	o		see A.1.9/8
6	per-recipient-fields	m	m	m	m		
6.1	actual-recipient-name	m	m	m	m		see A.1.10
6.2	delivery	m	m	m	m		
6.2.1	message-delivery-time	m	m	m	m		
6.2.2	type-of-MTS-user	m	m	m	m		
6.3	non-delivery	m	m	m	m		
6.3.1	non-delivery-reason-code	m	m	m	m		
6.3.2	non-delivery-diagnostic-code	o	m	m	m		
6.4	converted-encoded-information-types	m	m	m	m		see A.1.8/3
6.5	originally-intended-recipient-name	m	m	m	m		see A.1.10
6.6	supplementary-information	o	o	o	m		
6.7	extensions						
6.7.1	redirection-history	o	o	m	m		
6.7.2	physical-forwarding-address	o	c1	o	o		
6.7.3	recipient-certificate	o	o	o	o		

6.7.4	proof-of-delivery	o	c1	o	c1		see A.1.9/6

c1 - if supported in message submission envelope then m else i

A.1.8 Common data types

Ref	Element	MTS-user		MTA		Support	Notes/References
		Base	Profile	Base	Profile		
1	MTSIdentifier						
1.1	global-domain-identifier	m	m	m	m		see A.1.8/2
1.2	local-identifier	m	m	m	m		
2	GlobalDomainIdentifier						
2.1	country-name	m	m	m	m		
2.2	administration-domain-name	m	m	m	m		
2.3	private-domain-identifier	o	m	o	m		
3	EncodedInformationTypes						
3.1	built-in-encoded-information-types	m	m	m	m		
3.2	(non-basic parameters)	o	o	o	o		
3.3	extended-encoded-information-types	o	m	o	m		
4	ContentType						
4.1	built-in	o	o	o	m		
4.2	extended	o	o	o	m		
5	PerMessageIndicators						
5.1	disclosure-of-other-recipients	o	o	m	m		
5.2	implicit-conversion-prohibited	m	m	m	m		
5.3	alternate-recipient-allowed	o	o	m	m		
5.4	content-return-request	o	o	o	o		
5.5	reserved	o	o	o	m-		in CCITT X.411 only
5.6	bit-5	o	o	o	m-		in CCITT X.411 only
5.7	bit-6	o	o	o	m-		in CCITT X.411 only
5.8	service-message	o	o	o	m-		in CCITT X.411 only

A.1.9 Extension data types

Ref	Element	MTS-user		MTA		Support	Notes/References
		Base	Profile	Base	Profile		
1	ExtensionField						
1.1	type	o	m	m	m		
1.1.1	standard-extension	m	m	m	m		
1.1.2	private-extension	o	o	o	m-		not in CCITT X.411
1.2	criticality	m	m	m	m		
1.3	value	m	m	m	m		
2	MessageOriginAuthenticationCheck						
2.1	algorithm-identifier	m	m	m	m		
2.2	content	m	m	m	m		
2.3	content-identifier	o	m	o	m		
2.4	message-security-label	o	m	o	m		see A.1.9/3
3	MessageSecurityLabel						
3.1	security-policy-identifier	o	o	o	m-		
3.2	security-classification	o	o	o	m-		
3.3	privacy-mark	o	o	o	m-		
3.4	security-categories	o	o	o	m-		
4	MessageToken						
4.1	token-type-identifier	m	m	m	m		
4.2	asymmetric-token	m	m	m	m		
4.2.1	signature-algorithm-identifier	m	m	m	m		
4.2.2	name	m	m	m	m		
4.2.3	time	m	m	m	m		
4.2.4	signed-data	o	o	o	m-		
4.2.4.1	content-confidentiality-algorithm-identifier	o	o	o	m-		

4.2.4.2	content-integrity-check	o	o	o	m-		
4.2.4.3	message-security-label	o	o	o	m-		see A.1.9/3
4.2.4.4	proof-of-delivery-request	o	o	o	m-		
4.2.4.5	message-sequence-number	o	o	o	m-		
4.2.5	encryption-algorithm-identifier	o	o	o	m-		
4.2.6	encrypted-data	o	o	o	m-		
4.2.6.1	content-confidentiality-key	o	o	o	m-		
4.2.6.2	content-integrity-check	o	o	o	m-		
4.2.6.3	message-security-label	o	o	o	m-		see A.1.9/3
4.2.6.4	content-integrity-key	o	o	o	m-		
4.2.6.5	message-sequence-number	o	o	o	m-		
5	ProbeOriginAuthenticationCheck						
5.1	algorithm-identifier	m	m	m	m		
5.2	content-identifier	o	m	o	m		
5.3	message-security-label	o	m	o	m		see A.1.9/3
6	ProofOfDelivery						
6.1	algorithm-identifier	m	m	m	m		
6.2	delivery-time	m	m	m	m		
6.3	this-recipient-name	m	m	m	m		see A.1.10
6.4	originally-intended-recipient-name	o	o	o	m		see A.1.10
6.5	content	m	m	m	m		
6.6	content-identifier	o	m	o	m		
6.7	message-security-label	o	m	o	m		see A.1.9/3
7	ProofOfSubmission						
7.1	algorithm-identifier	m	m	m	m		
7.2	message-submission-envelope	m	m	m	m		
7.3	content	m	m	m	m		
7.4	message-submission-identifier	m	m	m	m		

7.5	message-submission-time	m	m	m	m		
8	ReportOriginAuthenticationCheck						
8.1	algorithm-identifier	m	m	m	m		
8.2	content-identifier	o	m	o	m		
8.3	message-security-label	o	m	o	m		see A.1.9/3
8.4	per-recipient	m	m	m	m		
8.4.1	actual-recipient-name	m	m	m	m		see A.1.10
8.4.2	originally-intended-recipient-name	o	m	o	m		see A.1.10
8.4.3	delivery	o	m	o	m		
8.4.3.1	message-delivery-time	m	m	m	m		
8.4.3.2	type-of-MTS-user	m	m	m	m		
8.4.3.3	recipient-certificate	o	m	o	m		
8.4.3.4	proof-of-delivery	o	m	o	m		see A.1.9/6
8.4.4	non-delivery	o	m	o	m		
8.4.4.1	non-delivery-reason-code	m	m	m	m		
8.4.4.2	non-delivery-diagnostic-code	o	m	o	m		

A.1.10 O/R names

Ref	**O/R Name Form**	**MTS-user**		**MTA**		**Support**	**Notes/References**
		Base	**Profile**	**Base**	**Profile**		
1	mnemonic O/R address	m	m	m	m-		see A.1.10.1
2	numeric O/R address	o	o	m	m-		see A.1.10.2
3	terminal O/R address	o	o	m	m-		see A.1.10.3
4	formatted postal O/R address	o	o	o	m-		see A.1.10.4
5	unformatted postal O/R address	o	o	o	m-		see A.1.10.5
6	directory-name	o	o	o	c1		

c1 - if the Designation of Recipient by Directory Name EoS is supported then m else if the O/R address is also present then m- else o

The following tables shall be completed according to the O/R address forms for which support is claimed above.

NOTE - Classification of an attribute as m for an MTA indicates only that its presence is required for the O/R address form.

A.1.10.1 Mnemonic O/R address

Ref	Element	MTS-user		MTA		Support	Notes/References
		Base	Profile	Base	Profile		
1	built-in-standard-attributes	m	m	m	m		
1.1	country-name	m	m	m	m		
1.2	administration-domain-name	m	m	m	m		
1.3	private-domain-name	o	m	o	m-		
1.4	organization-name	o	m	o	m-		
1.5	personal-name	o	m	o	m-		
1.5.1	surname	m	m	m	m		
1.5.2	given-name	o	m	o	m-		
1.5.3	initials	o	m	o	m-		
1.5.4	generation-qualifier	o	m	o	m-		
1.6	organizational-unit-names	o	m	o	m-		
2	built-in-domain-defined-attributes	o	m	o	m-		
3	extension-attributes	o	m	o	m-		
3.1	common-name	o	m	o	m-		
3.2	teletex-common-name	o	m	o	m-		
3.3	teletex-organization-name	o	m	o	m-		
3.4	teletex-personal-name	o	m	o	m-		
3.4.1	surname	m	m	m	m		
3.4.2	given-name	o	m	o	m-		
3.4.3	initials	o	m	o	m-		
3.4.4	generation-qualifier	o	m	o	m-		
3.5	teletex-organizational-unit-names	o	m	o	m-		
3.6	teletex-domain-defined-attributes	o	m	o	m-		

A.1.10.2 Numeric O/R address

Ref	Element	MTS-user		MTA		Support	Notes/References
		Base	Profile	Base	Profile		

1	built-in-standard-attributes	m	m	m	m		
1.1	country-name	m	m	m	m		
1.2	administration-domain-name	m	m	m	m		
1.3	private-domain-name	o	m	o	m-		
1.4	numeric-user-identifier	m	m	m	m		
2	built-in-domain-defined-attributes	o	m	o	m-		
3	extension-attributes	o	m	o	m-		
3.1	teletex-domain-defined-attributes	o	m	o	m-		

A.1.10.3 Terminal O/R address

Ref	Element	MTS-user		MTA		Support	Notes/References
		Base	Profile	Base	Profile		
1	built-in-standard-attributes	m	m	m	m		
1.1	country-name	o	m	o	m-		
1.2	administration-domain-name	o	m	o	m-		
1.3	network-address	m	m	m	m		
1.4	terminal-identifier	o	m	o	m-		
1.5	private-domain-name	o	m	o	m-		
2	built-in-domain-defined-attributes	o	m	o	m-		
3	extension-attributes	o	m	o	m-		
3.1	extended-network-address	m	m	m	m		
3.1.1	e163-4-address	o	o	o	m-		
3.1.2	psap-address	o	o	o	m-		
3.2	terminal-type	o	m	o	m-		
3.3	teletex-domain-defined-attributes	o	m	m	m		

A.1.10.4 Formatted postal O/R address

Ref	Element	MTS-user		MTA		Support	Notes/References
		Base	Profile	Base	Profile		
1	built-in-standard-attributes	m	m	m	m		
1.1	country-name	m	m	m	m		
1.2	administration-domain-name	m	m	m	m		
1.3	private-domain-name	o	m	o	m-		
2	extension-attributes	m	m	m	m		
2.1	physical-delivery-country-name	m	m	m	m		
2.2	physical-delivery-office-name	o	m	o	m-		
2.3	physical-delivery-office-number	o	m	o	m-		
2.4	physical-delivery-organization-name	o	m	o	m-		

2.5	physical-delivery-personal-name	o	m	o	m-		
2.6	postal-code	m	m	m	m		
2.7	poste-restante-address	o	m	o	m-		
2.8	post-office-box-address	o	m	o	m-		
2.9	pds-name	o	m	o	m-		
2.10	street-address	o	m	o	m-		
2.11	unique-postal-name	o	m	o	m-		
2.12	extension-OR-address-components	o	m	o	m-		
2.13	extension-physical-delivery-address-components	o	m	o	m-		
2.14	local-postal-attributes	o	m	o	m-		

A.1.10.5 Unformatted postal O/R address

Ref	**Element**	**MTS-user**		**MTA**		**Support**	**Notes/References**
		Base	**Profile**	**Base**	**Profile**		
1	built-in-standard-attributes	m	m	m	m		
1.1	country-name	m	m	m	m		
1.2	administration-domain-name	m	m	m	m		
1.3	private-domain-name	o	m	o	m-		
2	extension-attributes	m	m	m	m		
2.1	unformatted-postal-address	m	m	m	m		
2.2	physical-delivery-country-name	m	m	m	m		
2.3	postal-code	m	m	m	m		
2.4	pds-name	o	m	o	m-		

A.2 Optional functional groups

The following requirements are additional to those specified in A.1 if support of the functional group is claimed.

A.2.1 Security (SEC)

The support requirements for all SEC classes are as specified in A.1 unless otherwise specified below. Elements classified as cC shall be treated as m if support of a confidential security class variant (SnC) is claimed, else as o.

A.2.1.1 Supported operations

Ref	Element	MTS-user			MTA		
		S0	S1	S2	S0	S1	S2
2.4	SubmissionControl				m	m	m

A.2.1.2 Operation arguments/results

A.2.1.2.1 MTS-bind

Ref	Element	MTS-user			MTA		
		S0	S1	S2	S0	S1	S2
1.3	initiator-credentials	mr	mr	mr	mr	mr	mr
1.3.1	simple		ix	ix		ix	ix
1.3.2	strong		mr	mr		mr	mr
1.3.2.1.4	signed-data		mr	mr		mr	mr
1.2.3	security-context		mr	mr		mr	mr
2.3	responder-credentials	mr	mr	mr	mr	mr	mr
2.3.1	simple		ix	ix		ix	ix
2.3.2	strong		mr	mr		mr	mr
2.3.2.1.4	signed-data		mr	mr		mr	mr

A.2.1.2.2 MessageSubmission

Ref	Element	UA			MTA		
		S0	S1	S2	S0	S1	S2
2.4.1	originating-MTA-certificate	ix	ix	o	ix	ix	o
2.4.2	proof-of-submission	ix	ix	m	ix	ix	m

A.2.1.2.3 SubmissionControl

Ref	Element	UA			MTA		
		S0	S1	S2	S0	S1	S2

1.1.2	permissible-operations				m	m	m
1.1.3	permissible-maximum-content-length				m	m	m
1.1.4	permissible-lowest-priority				m	m	m
1.1.5	permissible-security-context		m	m		m	m

A.2.1.2.5 MessageDelivery

Ref	Element	MTS-user			MTA		
		S0	S1	S2	S0	S1	S2
2.2	proof-of-delivery	m	m	m	m	m	m

A.2.1.2.6 DeliveryControl

Ref	Element	MTS-user			MTA		
		S0	S1	S2	S0	S1	S2
1.1.5	permissible-security-context		m	m		m	m

A.2.1.2.7 Register

Ref	Element	UA			MTA		
		S0	S1	S2	S0	S1	S2
1.1	user-name		m	m		m	m
1.7.1	user-security-label		m	m		m	m

A.2.1.2.8 ChangeCredentials

Ref	Element	UA			MTA		
		S0	S1	S2	S0	S1	S2
1.1.1	simple		ix	ix		ix	ix
1.1.2	strong		m	m		m	m
1.2.1	simple		ix	ix		ix	ix
1.2.2	strong		m	m		m	m

A.2.1.3 MessageSubmissionEnvelope

Ref	Element	UA			MTA		
		S0	S1	S2	S0	S1	S2
8.6	originator-certificate				m-	m-	m-

8.7	content-confidentiality-algorithm-identifier	cC	cC	cC	m-	m-	m-
8.8	message-origin-authentication-check			mr	m-	m-	mr
8.9	message-security-label		mr	mr	m-	mr	mr
8.10	proof-of-submission-request			m			m
9.4.10	message-token	m	mr	mr	m-	mr	mr
9.4.11	content-integrity-check	m	m	m	m-	m-	m-
9.4.12	proof-of-delivery-request	m	m	m	m	m	m

A.2.1.4 ProbeSubmissionEnvelope

Ref	Element	UA			MTA		
		S0	S1	S2	S0	S1	S2
7.4	originator-certificate				m-	m-	m-
7.5	message-security-label		mr	mr	m-	mr	mr
7.7	probe-origin-authentication-check			mr	m-	m-	mr

A.2.1.5 MessageDeliveryEnvelope

Ref	Element	MTS-user			MTA		
		S0	S1	S2	S0	S1	S2
3.12.11	originator-certificate				m-	m-	m-
3.12.12	message-token	m	mr	mr	m-	mr	mr
3.12.13	content-confidentiality-algorithm-identifier	cC	cC	cC	m-	m-	m-
3.12.14	content-integrity-check	m	m	m	m-	m-	m-
3.12.15	message-origin-authentication-check			mr	m-	m-	mr
3.12.16	message-security-label		mr	mr	m-	mr	mr
3.12.17	proof-of-delivery-request	m	m	m	m	m	m

A.2.1.6 ReportDeliveryEnvelope

Ref	Element	MTS-user			MTA		
		S0	S1	S2	S0	S1	S2
5.1	message-security-label		mr	mr	m-	mr	mr
5.5	reporting-MTA-certificate				m-	m-	m-
5.6	report-origin-authentication-check			mr	m-	m-	mr
6.7.3	recipient-certificate				m-	m-	m-
6.7.4	proof-of-delivery	m	m	m	m	m	m

A.2.1.7 Extension data types

Ref	Element	MTS-user			MTA		
		S0	S1	S2	S0	S1	S2
2	MessageOriginAuthenticationCheck						
2.4	message-security-label		mr	mr		mr	mr
3	MessageSecurityLabel						
3.1	security-policy-identifier		mr	mr		mr	mr
3.2	security-classification		m	m		m	m
3.3	security-categories		m	m		m	m
4	MessageToken						
4.2.4	signed-data	m	m	m	m	m	m
4.2.4.1	content-confidentiality-algorithm-identifier	cC	cC	cC	m-	m-	m-
4.2.4.2	content-integrity-check	m	m	m	m	m	m
4.2.4.3	message-security-label		m	m		m	m
4.2.4.4	proof-of-delivery-request	m	m	m	m	m	m
4.2.5	encryption-algorithm-identifier		m	m		m	m
4.2.6	encrypted-data		m	m		m	m
4.2.6.2	content-integrity-check	m	m	m	m	m	m
4.2.6.3	message-security-label		m	m		m	m
5	ProbeOriginAuthenticationCheck						
5.3	message-security-label		mr	mr		mr	mr
6	ProofOfDelivery						
6.7	message-security-label		mr	mr		mr	mr
7	ReportOriginAuthenticationCheck						
7.3	message-security-label		mr	mr		mr	mr

A.2.2 Physical Delivery (PD)

The support requirements specified below are for a UA and for an MTA on submission, and for an MTA with a co-located PDAU on delivery, as appropriate.

A.2.2.1 MessageSubmissionEnvelope

Ref	Element	Profile	
		UA	MTA
8.5	originator-return-address		m
9.4.3	physical-forwarding-prohibited	m	m
9.4.4	physical-forwarding-address-request		m
9.4.5	physical-delivery-modes	m	m
9.4.6	registered-mail-type		m
9.4.7	recipient-number-for-advice		m
9.4.8	physical-rendition-attributes		m
9.4.9	physical-delivery-report-request		m

A.2.2.2 ProbeSubmissionEnvelope

Ref	Element	Profile	
		UA	MTA
8.4.3	physical-rendition-attributes		m

A.2.2.3 MessageDeliveryEnvelope

Ref	Element	Profile	
		PDAU	MTA
3.12.3	physical-forwarding-prohibited	m	m
3.12.5	physical-delivery-modes		m
3.12.8	physical-rendition-attributes		m
3.12.10	physical-delivery-report-request		m

A.2.2.4 ReportDeliveryEnvelope

Ref	Element	Profile	
		MTS-user	MTA

6.7.2	physical-forwarding-address		m

A.2.2.5 O/R names

Ref	O/R Address Form	Profile	
		MTS-user	MTA
4	formatted postal O/R address	m	m
5	unformatted postal O/R address	m	m

A.2.3 Conversion (CV)

A.2.3.1 MessageSubmissionEnvelope

Ref	Element	Profile	
		UA	MTA
9.3	explicit-conversion		c1

c1 - if implicit conversion is not supported then m

A.2.3.2 ProbeSubmissionEnvelope

Ref	Element	Profile	
		UA	MTA
8.3	explicit-conversion		c1

c1 - if implicit conversion is not supported then m

A.2.4 Redirection (RED)

A.2.4.1 MessageSubmissionEnvelope

Ref	Element	Profile	
		UA	MTA
9.4.1	originator-requested-alternate-recipient		m

A.2.4.2 ProbeSubmissionEnvelope

Ref	Element	Profile	
		UA	MTA
8.4.1	originator-requested-alternate-recipient		m

A.2.5 Latest Delivery (LD)

A.2.5.1 MessageSubmissionEnvelope

Ref	Element	Profile	
		UA	MTA
8.4	latest-delivery-time	m	m

A.2.6 Return of Contents (RoC)

A.2.6.1 Operation arguments/results

A.2.6.1.1 Report Delivery

Ref	Element	Profile	
		MTS-user	MTA
1.2	returned-content	m	m

A.2.6.2 Common data types

Ref	Element	Profile	
		UA	MTA
5	PerMessageIndicators		

5.4	content-return-request	m	m

A.2.7 Use of Directory (DIR)

A.2.7.1 O/R names

Ref	O/R Name Form	Profile	
		MTS-user	MTA
6	directory-name	m	m

A.3 Additional information

A.3.1 Content types supported

The following table shall be completed to indicate (Y or 3) which content type(s) the implementation can support on submission and delivery (see clause 6 of ISO/IEC ISP 10611-1). Any differences between support on submission and support on delivery shall be indicated in the Comments column.

Ref	Content Type	Supported	Comments
1	built-in		
1.1	unidentified (0)		
1.2	interpersonal-messaging-1984 (2)		
1.3	interpersonal-messaging-1988 (22)		
1.4	(EDI messaging) (35)		
2	extended (specify)		

A.3.2 Encoded information types supported

The following table shall be completed to indicate (Y or 3) which encoded information type(s) the implementation can support on submission and delivery (see clause 6 of ISO/IEC ISP 10611-1). Any differences between support on submission and support on delivery shall be indicated in the Comments column.

Ref	Encoded Information Type	Supported	Comments
1	built-in		
1.1	undefined (0)		
1.2	ia5-text (2)		
1.3	g3-facsimile (3)		
1.4	g4-class-1 (4)		
1.5	teletex (5)		
1.6	videotex (6)		
1.7	voice (7)		
1.8	mixed-mode (9)		
1.9	other (specify)		
2	extended (specify)		

A.3.3 Encoded information type conversions supported

The following table shall be completed for an MTA if support of the Conversion FG is claimed, to indicate (Y or 3) which encoded information type conversions the implementation can perform (see clause 7.1 of ISO/IEC ISP 10611-1). The supplier shall also state in the Comments column for which content types support of the conversion capability is claimed and under what conditions loss of information is determined (if applicable).

Ref	Encoded Information Type Conversion	Supported	Comments
1	explicit-conversion		
1.1	ia5-text-to-teletex (0)		
1.2	ia5-text-to-g3-facsimile (8)		
1.3	ia5-text-to-g4-class-1 (9)		
1.4	ia5-text-to-videotex (10)		
1.5	teletex-to-ia5-text (11)		
1.6	teletex-to-g3-facsimile (12)		
1.7	teletex-to-g4-class-1 (13)		
1.8	teletex-to-videotex (14)		
1.9	videotex-to-ia5-text (16)		
1.10	videotex-to-teletex (17)		
2	implicit conversion (specify)		

Annex B

(normative)

Amendments and corrigenda

International Standards are subject to constant review and revision by the ISO/IEC Technical Committees concerned. The following amendments and corrigenda are approved by ISO/IEC JTC1 and are considered as normative references in this part of ISO/IEC ISP 10611.

NOTE - Corresponding corrigenda to the equivalent CCITT Recommendations are contained in the joint CCITT/ISO MHS Implementor's Guide.

MOTIS

ISO/IEC 10021-1/Cor.1:1991

ISO/IEC 10021-1/Cor.2:1991

ISO/IEC 10021-1/Cor.3:1992

ISO/IEC 10021-1/Cor.4:1992

ISO/IEC 10021-1/Cor.5:1992

ISO/IEC 10021-2/Cor.1:1991

ISO/IEC 10021-2/Cor.2:1991

ISO/IEC 10021-2/Cor.3:1992

ISO/IEC 10021-2/Cor.4:1992

ISO/IEC 10021-4/Cor.1:1991

ISO/IEC 10021-4/Cor.2:1991

ISO/IEC 10021-4/Cor.3:1992

ISO/IEC 10021-4/Cor.4:1992

ISO/IEC 10021-4/Cor.5:1992

ISO/IEC 10021-6/Cor.1:1991

ISO/IEC 10021-6/Cor.2:1991

ISO/IEC 10021-6/Cor.3:1992

ISO/IEC 10021-6/Cor.4:1992

ISO/IEC 10021-6/Cor.5:1992

TITLE: Information technology - International Standardized Profiles AMH1n -
Message Handling Systems - Common Messaging -
Part 5 : AMH13 - MS Access (P7)

SOURCE: Project Editor (Jon Stranger, UK)

STATUS: DISP text, 1993-7-31

This document forms part of a proposed multipart ISP for MHS covering Common Messaging requirements (AMH1), as identified in the Taxonomy for International Standardized Profiles (ISO/IEC TR 10000-2 : 1992).

This revised DISP version reflects resolution of all remaining outstanding issues at the 6th MHS ISP Special Group (MISG) meeting (Kyoto, February 1-4, 1993) together with some editorial and minor errata which have been determined since submission to ISO/IEC JTC1/SGFS. The content of this document is considered by the MHS expert groups of the three regional workshops as harmonized.

The technical content of this document has been derived wherever possible from the existing EWOS/ETSI and OIW regional profiles in this area. However, differences between the content of this document and one or more regional profiles may exist.

Contents

Annexes

ISO/IEC Copyright Office _ Case Postale 56 _ CH-1211 Genève 20 _ Switzerland

Printed in Switzerland

Foreword

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

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC1. In addition to developing International Standards, ISO/IEC JTC1 has created a Special Group on Functional Standardization for the elaboration of International Standardized Profiles.

An International Standardized Profile is an internationally agreed, harmonized document which identifies a standard or group of standards, together with options and parameters, necessary to accomplish a function or set of functions.

Draft International Standardized Profiles are circulated to national bodies for voting. Publication as an International Standardized Profile requires approval by at least 75% of the national bodies casting a vote.

International Standardized Profile ISO/IEC ISP 10611-5 was prepared with the collaboration of:

- Asia-Oceania Workshop (AOW)

- European Workshop for Open Systems (EWOS) [jointly with the

European Telecommunications Standards Institute (ETSI)]

- OSE Implementors' Workshop (OIW)

ISO/IEC ISP 10611 consists of the following parts, under the general title *Information technology - International Standardized Profiles AMH1n - Message Handling Systems - Common Messaging*:

- Part 1 : MHS Service Support

- Part 2 : Specification of ROSE, RTSE, ACSE, Presentation and Session Protocols for use by MHS

- Part 3 : AMH11 - Message Transfer (P1)

- Part 4 : AMH12 - MTS Access (P3)

- Part 5 : AMH13 - MS Access (P7)

This part of ISO/IEC ISP 10611 contains two annexes, A and B, which are normative.

Introduction

This part of International Standardized Profile ISO/IEC ISP 10611 is defined within the context of Functional Standardization, in accordance with the principles specified by ISO/IEC TR 10000, “Framework and Taxonomy of International Standardized Profiles”. The context of Functional Standardization is one part of the overall field of Information Technology (IT) standardization activities, covering base standards, profiles, and registration mechanisms. A profile defines a combination of base standards that collectively perform a specific well-defined IT function. Profiles standardize the use of options and other variations in the base standards, and provide a basis for the development of uniform, internationally recognized system tests.

One of the most important rôles for an ISP is to serve as the basis for the development (by organizations other than ISO and IEC) of internationally recognized tests and test centres. ISPs are produced not simply to ‘legitimize' a particular choice of base standards and options, but to promote real system interoperability. The development and widespread acceptance of tests based on this and other ISPs is crucial to the successful realization of this goal.

The text for this part of ISO/IEC ISP 10611 was developed in close cooperation between the MHS Expert Groups of the three Regional Workshops: the North American OSE Implementors' Workshop (OIW), the European Workshop for Open Systems (EWOS) (jointly with the corresponding expert group of the European Telecommunications Standards Institute - ETSI) and the OSI Asia-Oceania Workshop (AOW). This part of ISO/IEC ISP 10611 is harmonized between these three Workshops and it has been ratified by the plenary assemblies of all three Workshops.

Information technology - International Standardized Profiles AMH1n - Message Handling Systems - Common Messaging

Part 5 : AMH13 - MS Access (P7)

1 Scope

1.1 General

This part of ISO/IEC ISP 10611 covers access to a message store (MS) using the P7 MS Access Protocol (see also figure 1). These specifications form part of the Common Messaging application functions, as defined in the parts of ISO/IEC ISP 10611, which form a common basis for content type-dependent International Standardized Profiles for MHS that will be developed.

1.2 Position within the taxonomy

This part of ISO/IEC ISP 10611 is the fifth part of a multipart ISP identified in ISO/IEC TR 10000-2 as “AMH1, Message Handling Systems - Common Messaging” (see also ISO/IEC TR 10000-1, 8.2 for the definition of multipart ISPs).

This part of ISO/IEC ISP 10611 specifies the following profile:

AMH13 - MS Access (P7)

The AMH13 profile may be combined with any T-Profiles (see ISO/IEC TR 10000) specifying the OSI connection-mode Transport service.

1.3 Scenario

The model used is one of access to a message store (MS) by an MS-user - specifically, the intercommunication between an MS and an MS-user (i.e., a user agent) using the P7 protocol, as shown in figure 1.

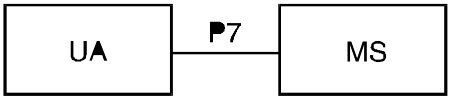


Figure 1 - AMH13 scenario

The AMH13 profile covers all aspects of the MS Abstract Service, as defined in ISO/IEC 10021-5, when realized using the P7 protocol.

The OSI upper layer services and protocols to support the Message Handling Systems functions covered by the AMH13 profile are specified in the set of standards identified in table 1.

Table 1 - AMH13 profile model

Application Layer	MHS	ISO/IEC 10021-6
	ROSE	see ISO/IEC ISP 10611-2
	RTSE	see ISO/IEC ISP 10611-2
	ACSE	see ISO/IEC ISP 10611-2
Presentation Layer		see ISO/IEC ISP 10611-2
Session Layer		see ISO/IEC ISP 10611-2

2 Normative references

The following documents contain provisions which, through reference in this text, constitute provisions of this part of ISO/IEC ISP 10611. At the time of publication, the editions indicated were valid. All documents are subject to revision, and parties to agreements based on this part of ISO/IEC ISP 10611 are warned against automatically applying any more recent editions of the documents listed below, since the nature of references made by ISPs to such documents is that they may be specific to a particular edition. Members of IEC and ISO maintain registers of currently valid International Standards and ISPs, and CCITT maintains published editions of its current Recommendations.

Amendments and corrigenda to the base standards referenced are listed in annex B.

NOTE - References in the body of this part of ISO/IEC 10611 to specific clauses of ISO/IEC documents shall be considered to refer also to the corresponding clauses of the equivalent CCITT Recommendations (as noted below) unless otherwise stated.

ISO/IEC TR 10000-1: 1992*, Information technology - Framework and taxonomy of International Standardized Profiles - Part 1: Framework.*

ISO/IEC TR 10000-2: 1992*, Information technology - Framework and taxonomy of International Standardized Profiles - Part 2: Taxonomy.*

ISO/IEC 10021-1: 1990*, Information technology - Text Communication - Message-Oriented Text Interchange Systems (MOTIS) - Part 1: Service Overview. [see also CCITT Recommendation X.400(1988)]*

ISO/IEC 10021-2: 1990*, Information technology - Text Communication - Message-Oriented Text Interchange Systems (MOTIS) - Part 2: Overall Architecture. [see also CCITT Recommendation X.402(1988)]*

ISO/IEC 10021-5: 1990*, Information technology - Text Communication - Message-Oriented Text Interchange Systems (MOTIS) - Part 5: Message Store: Abstract Service Definition. [see also CCITT Recommendation X.413(1988)]*

ISO/IEC 10021-6: 1990*, Information technology - Text Communication - Message-Oriented Text Interchange Systems (MOTIS) - Part 6: Protocol Specifications. [see also CCITT Recommendation X.419(1988)]*

ISO/IEC ISP 10611-1: ---[2]*, Information technology - International Standardized Profiles AMH1n - Message Handling Systems - Common Messaging - Part 1: MHS Service Support.*

ISO/IEC ISP 10611-2: ---[1]*, Information technology - International Standardized Profiles AMH1n - Message Handling Systems - Common Messaging - Part 2: Specification of ROSE, RTSE, ACSE, Presentation and Session Protocols for use by MHS.*

CCITT Recommendation X.400(1988)*, Message handling system and service overview.*

CCITT Recommendation X.402(1988)*, Message handling systems: Overall architecture.*

[2] To be published.

CCITT Recommendation X.413(1988), *Message handling systems: Message store: Abstract service definition.*

CCITT Recommendation X.419(1988), *Message handling systems: Protocol specifications.*

MHS Implementors' Guide, Version 8, March 1992 (CCITT Special Rapporteur's Group on Message Handling Systems and ISO/IEC JTC1/SC18/WG4 SWG on Messaging).

3 Definitions

For the purposes of this part of ISO/IEC ISP 10611, the following definitions apply.

Terms used in this part of ISO/IEC ISP 10611 are defined in the referenced base standards; in addition, the following terms are defined.

3.1 General

Basic requirement : an Element of Service, protocol element, procedural element or other identifiable feature specified in the base standards which is required to be supported by all MHS implementations.

Functional group : a specification of one or more related Elements of Service, protocol elements, procedural elements or other identifiable features specified in the base standards which together support a significant optional area of MHS functionality.

NOTE - A functional group can cover any combination of MHS features specified in the base standards for which the effect of implementation can be determined at a standardized external interface - i.e., via a standard OSI communications protocol (other forms of exposed interface, such as a standardized programmatic interface, are outside the scope of this version of ISO/IEC ISP 10611).

3.2 Support classification

To specify the support level of operations, arguments, results, attributes and other protocol features for this part of ISO/IEC ISP 10611, the following terminology is defined.

3.2.1 Static capability

The following classifications are used in this part of ISO/IEC ISP 10611 to specify static conformance requirements - i.e., capability.

In the case of arguments and results (protocol elements), the classification is relative to that of the containing element, if any. Where the constituent elements of a non-primitive element are not individually specified, then each shall be considered to have the classification of that element. Where the range of values to be supported for an element is not specified, then all values defined in the MHS base standards shall be supported.

mandatory support (**m**) : the element or feature shall be fully supported. An implementation shall be able to generate the element, and/or receive the element and perform all associated procedures (i.e., implying the ability to handle both the syntax and the semantics of the element) as relevant, as specified in the MHS base standards. Where support for origination (generation) and reception are not distinguished, then both capabilities shall be assumed. Mandatory support of an MS attribute requires that it is supported in the context of all applicable supported operation arguments and results and also for use within a selector to the level of support claimed for the filter item. The way in which attribute values are stored by an MS implementation, or used by a UA implementation, is otherwise a local matter.

optional support (**o**) : an implementation is not required to support the element or feature. If support is claimed, the element shall be treated as if it were specified as mandatory support. If support is not claimed, and the element is an argument, then an implementation shall generate an appropriate error if the element is received. If support is not claimed, and the element is a result, then an implementation may ignore the element if it is received.

conditional support (**c**) : the element shall be supported under the conditions specified in this part of ISO/IEC ISP 10611. If these conditions are met, the element shall be treated as if it were specified as mandatory support. If these conditions are not met, the element shall be treated as if it were specified as optional support (unless otherwise stated).

out of scope (**i**) : the element is outside the scope of this part of ISO/IEC ISP 10611 - i.e., it will not be the subject of an ISP conformance test.

not applicable (**–**) : the element is not applicable in the particular context in which this classification is used.

3.2.2 Dynamic behaviour

The above classifications are used in this part of ISO/IEC ISP 10611 to specify static conformance requirements (i.e., capability); dynamic conformance requirements (i.e., behaviour) are as specified in the MHS base standards. However, in a few cases it has been necessary to specify additional dynamic conformance requirements in this profile. These are specified using a second classification code for an element, as follows.

NOTE - Clause 6.7 of ISO/IEC TR 10000-1 states that a profile shall not introduce a constraint on dynamic behaviour on reception. However, in the case of MHS security (at least), the base standards define a suitable error indication to cover the breach of a security policy but do not specify the precise conditions under which such error indication shall be used. Any such specification in a profile is thus a legitimate qualification of the base standards rather than a modification of such provisions.

required (**r**) : the element shall always be present. An implementation shall ensure that the element is always generated or otherwise used, as appropriate. Absence of the element on reception shall result in termination or rejection of the communication with an appropriate error indication as specified in the MHS base standards.

excluded (**x**) : the element shall never be present. An implementation shall ensure that the element is never generated or otherwise used, as appropriate. Presence of the element on reception shall result in termination or rejection of the communication with an appropriate error indication as specified in the MHS base standards.

NOTE - It is recognized that some implementations may be required to exclude even a static capability in such cases, but such considerations are outside the scope of this profile. Any elements which are specified as excluded (x) in this profile are thus also specified as out of scope (i) in terms of static capability.

4 Abbreviations

AMH	Application Message Handling
ASN.1	Abstract Syntax Notation One
DIR	Use of Directory
EoS	Element of Service
FG	Functional group
ISP	International Standardized Profile
MHS	Message Handling Systems
MS	Message store
MTA	Message transfer agent

OSI	Open Systems Interconnection
PD	Physical Delivery
SEC	Security
UA	User agent

Support level for protocol elements and features (see 3.2):

m	mandatory support
o	optional support
c	conditional support
i	out of scope
–	not applicable
r	required
x	excluded

5 Conformance

This part of ISO/IEC ISP 10611 states requirements upon implementations to achieve interworking. A claim of conformance to this part of ISO/IEC ISP 10611 is a claim that all requirements in the relevant base standards are satisfied, and that all requirements in the following clauses and in annex A of this part of ISO/IEC ISP 10611 are satisfied. Annex A states the relationship between these requirements and those of the base standards.

5.1 Conformance statement

For each implementation claiming conformance to profile AMH13 as specified in this part of ISO/IEC ISP 10611, a PICS shall be made available stating support or non-support of each option identified in this part of ISO/IEC ISP 10611.

The scope of conformance to profile AMH13 covers both MSs and MS-users (i.e., UAs). A claim of conformance to profile AMH13 shall state whether the implementation claims conformance as an MS or as an MS-user.

5.2 MHS conformance

This part of ISO/IEC ISP 10611 specifies implementation options or selections such that conformant implementations will satisfy the conformance requirements of ISO/IEC 10021 and the CCITT X.400 Recommendations.

Implementations conforming to profile AMH13 as specified in this part of ISO/IEC ISP 10611 shall implement all the mandatory support (m) features identified as basic requirements in annex A and shall state which optional support (o) features are implemented. They shall also support corresponding MHS Elements of Service and associated procedures as specified in ISO/IEC ISP 10611-1, as appropriate to the scope of this profile and to the role (i.e., MS or MS-user) for which conformance is claimed.

Implementations conforming to profile AMH13 as specified in this part of ISO/IEC ISP 10611 shall state whether or not they support any of the optional functional groups as specified in ISO/IEC ISP 10611-1 which are applicable to the scope of this profile and to the role (i.e., MS or MS-user) for which conformance is claimed. For each functional group for which support is claimed, an implementation shall implement all the mandatory support (m) features identified for that functional group in annex A and shall state which optional support (o) features are implemented. They shall also support corresponding MHS Elements of Service and associated procedures as specified in ISO/IEC ISP 10611-1, as appropriate to the scope of this profile and to the role (i.e., MS or MS-user) for which conformance is claimed.

Implementations conforming to profile AMH13 as specified in this part of ISO/IEC ISP 10611 shall state the P7 application context(s) for which conformance is claimed.

5.3 Underlying layers conformance

Implementations conforming to profile AMH13 as specified in this part of ISO/IEC ISP 10611 shall also conform to ISO/IEC ISP 10611-2 in accordance with the P7 application context(s) for which conformance is claimed.

Annex A[3]

(normative)

ISPICS Proforma

for ISO/IEC ISP 10611-5 (AMH13)

In the event of a discrepancy becoming apparent in the body of this part of ISO/IEC ISP 10611 and the tables in this annex, this annex is to take precedence.

[**Editor's Note** : It had been intended that this annex would eventually be based on the ISO/IEC 10021 P7 PICS proforma. However, the current version of the latter (as contained in ISO/IEC CD 10021-14) is defective and the whole ISO/IEC work item for the development of MOTIS PICS proformas has now been suspended. As a result, it has been necessary to turn the P7 IPRL in this annex into a complete ISPICS (the alternative approach of a separate annex containing the assumed base standard PICS proforma was not considered appropriate in this case). This annex broadly follows the final draft of CCITT Recommendation X.484 (April 1992), but the structure has been modified to some extent to take account of profiling requirements and the somewhat different conformance objectives.]

Clause A.1 specifies the basic requirements for conformance to profile AMH13. Clause A.2 specifies additional requirements to those specified in A.1 for each of the optional functional groups if conformance to such a functional group is claimed. Clause A.3 allows additional information to be provided for certain aspects of an implementation where no specific requirements are included in ISO/IEC ISP 10611. All three clauses shall be completed as appropriate.

In each table, the "Base" column reflects the level of support required for conformance to the base standard and the "Profile" column specifies the level of support required by this ISP (using the classification and notation defined in 3.2).

[**Editor's Note** : The identification of the base standard requirement has in some cases had to be interpreted or varied from that specified in the current CCITT PICS proforma, either due to the different classification scheme employed or where the base standard is unclear and it has been considered that the CCITT PICS proforma is in error.]

The Support column is provided for completion by the supplier of the implementation as follows:

Y	the element or feature is fully supported (i.e., satisfying the requirements of the m profile support classification)
N	the element or feature is not supported, further qualified to indicate the action taken on receipt of such an element as follows: ND - the element is discarded/ignored NR - the PDU is rejected (with an appropriate error indication where applicable)

[3] **Copyright release for ISPICS proformas**
Users of this International Standardized Profile may freely reproduce the ISPICS proforma in this annex so that it can be used for its intended purpose and may further publish the completed ISPICS.

– or blank	the element or feature is not applicable (i.e., a major feature or composite protocol element which includes this element or feature is not supported)

Identification of the implementation

Identification of PICS

Ref	Question	Response
1	Date of statement (DD/MM/YY)	
2	PICS serial number	
3	System conformance statement cross reference	

Identification of IUT

Ref	Question	Response
1	Implementation name	
2	Implementation version	
3	Machine name	
4	Machine version	
5	Operating system name	
6	Operating system version	
7	Special configuration	
8	Other information	

Identification of supplier

Ref	Question	Response
1	Organization name	
2	Contact name(s)	
3	Address	
4	Telephone number	
5	Telex number	
6	Fax number	
7	E-mail address	
8	Other information	

Identification of protocol

Ref	Question	Response
1	Title, reference number and date of publication of the protocol standard	
2	Protocol version(s)	
3	Addenda/amendments/corrigenda implemented	
4	Defect reports implemented	

Type of implementation

Ref	Implementation Type	Response
1	MS-user (UA)	
2	MS (co-located with MTA)	
3	MS (P3 interface to MTA)	

NOTE - A separate PICS shall be completed for each implementation type for which conformance is claimed.

Global statement of conformance

Ref	Question	Response
1	Are all mandatory base standards requirements implemented?	

Statement of profile conformance

Ref	Question	Response	Comments
1	Are all mandatory requirements of profile AMH13 implemented?		
2	Are all mandatory requirements of any of the following optional functional groups implemented?		
2.1	Security (SEC)		class(es):
2.2	Physical Delivery (PD)		
2.3	Latest Delivery (LD)		
2.4	Return of Contents (RoC)		
2.8	Use of Directory (DIR)		

A.1 Basic requirements

A.1.1 Supported application contexts

Ref	Application Context	UA		MS		Support	Notes/References
		Base	Profile	Base	Profile		
1	ms-access	m	m	m	m		
2	ms-reliable-access	o	o	o	o		

A.1.2 Supported operations

A.1.2.1 Bind and Unbind

Ref	Operation	UA		MS		Support	Notes/References
		Base	Profile	Base	Profile		
1	MSBInd	m	m	m	m		see A.1.3.1
2	MSUnbind	m	m	m	m		

A.1.2.2 Message Submission Service Element (MSSE)

Ref	Operation	UA		MS		Support	Notes/References
		Base	Profile	Base	Profile		
1	MessageSubmission	m	m	m	m		see A.1.3.2
2	ProbeSubmission	o	o	m	m		see A.1.3.3
3	CancelDeferredDelivery	o	o	m	m		see A.1.3.4
4	SubmissionControl	m	m	o	c1		see A.1.3.5

c1 - if the MS has a P3 interface to the MTA then m else if supported by the MTA then m else o

NOTE - An MS is only required to be able to copy the syntax of the arguments and results of these operations to the MTA or UA, as appropriate; it is not required to be able to originate such elements or to take any explicit action based on the semantics of such elements.

A.1.2.3 Message Retrieval Service Element (MRSE)

Ref	Operation	UA		MS		Support	Notes/References
		Base	Profile	Base	Profile		
1	Summarize	o	o	m	m		see A.1.3.6
2	List	o	o	m	m		see A.1.3.7
3	Fetch	m	m	m	m		see A.1.3.8
4	Delete	m	m	m	m		see A.1.3.9
5	Register-MS	o	o	m	m		see A.1.3.10
6	Alert	o	o	o	o		see A.1.3.11

A.1.2.4 Message Administration Service Element (MASE)

Ref	Operation	UA		MS		Support	Notes/References
		Base	Profile	Base	Profile		
1	Register	o	o	o	m		see A.1.3.12
2	ChangeCredentials (MTA to UA)	o	o	o	c1		see A.1.3.13
3	ChangeCredentials (UA to MTA)	o	o	o	m		see A.1.3.13

c1 - if the MS has a P3 interface to the MTA then m else if supported by the MTA then m else o

NOTE - An MS is only required to be able to copy the syntax of the arguments and results of these operations to the MTA or UA, as appropriate; it is not required to be able to originate such elements or to take any explicit action based on the semantics of such elements. For a UA, some or all of the services and functionality supported by these operations may be implemented by other means as a local matter.

A.1.3 Operation arguments/results

A.1.3.1 MS-bind

Ref	Element	UA		MS		Support	Notes/References
		Base	Profile	Base	Profile		
1	ARGUMENT						
1.1	initiator-name	m	m	m	m		
1.2	initiator-credentials	m	m	m	m		
1.2.1	simple	m	m	m	m		
1.2.1.1	IA5String	o	o	m	m		
1.2.1.2	OCTET STRING	o	m	m	m		
1.2.2	strong	o	o	o	o		
1.2.2.1	bind-token	m	m	m	m		
1.2.2.1.1	signature-algorithm-identifier	m	m	m	m		
1.2.2.1.2	name	m	m	m	m		
1.2.2.1.3	time	m	m	m	m		
1.2.2.1.4	signed-data	o	o	o	o		
1.2.2.1.5	encryption-algorithm-identifier	o	o	o	o		
1.2.2.1.6	encrypted-data	o	o	o	o		
1.2.2.2	certificate	o	o	o	o		
1.3	security-context	o	o	o	o		see A.1.9/3
1.4	fetch-restrictions	o	o	o	o		
1.4.1	allowed-content-types	o	o	o	o		
1.4.2	allowed-EITs	o	o	o	o		
1.4.3	maximum-content-length	o	o	o	o		
1.5	ms-configuration-request	o	o	o	m		
2	RESULT						
2.1	responder-credentials	m	m	m	m		
2.1.1	simple	m	m	m	m		
2.1.1.1	IA5String	m	m	o	o		

2.1.1.2	OCTET STRING	m	m	o	m		
2.1.2	strong	o	o	o	o		
2.1.2.1	bind-token	m	m	m	m		
2.1.2.1.1	signature-algorithm-identifier	m	m	m	m		
2.1.2.1.2	name	m	m	m	m		
2.1.2.1.3	time	m	m	m	m		
2.1.2.1.4	signed-data	o	o	o	o		
2.1.2.1.5	encryption-algorithm-identifier	o	o	o	o		
2.1.2.1.6	encrypted-data	o	o	o	o		
2.2	available-auto-actions	o	o	m	m		
2.2.1	auto-alert	o	o	o	o		
2.2.2	auto-forward	o	o	o	o		
2.3	available-attribute-types	o	o	m	m		
2.4	alert-indication	o	o	o	o		
2.5	content-types-supported	o	o	m	m		

A.1.3.2 MessageSubmission

Ref	**Element**	**UA**		**MS**		**Support**	**Notes/References**
		Base	**Profile**	**Base**	**Profile**		
1	ARGUMENT						
1.1	envelope	m	m	m	m		see A.1.4
1.2	content	m	m	m	m		
2	RESULT						
2.1	message-submission-identifier	m	m	m	m		see A.1.8/8
2.2	message-submission-time	m	m	m	m		
2.3	content-identifier	o	c1	m	m		
2.4	extensions						
2.4.1	originating-MTA-certificate	o	i	o	i		
2.4.2	proof-of-submission	o	i	o	i		see A.1.9/6

c1 - if supported in message submission envelope then m else –

A.1.3.3 ProbeSubmission

Ref	Element	UA		MS		Support	Notes/References
		Base	Profile	Base	Profile		
1	ARGUMENT						
1.1	envelope	m	m	m	m		see A.1.5
2	RESULT						
2.1	probe-submission-identifier	m	m	m	m		see A.1.8/8
2.2	probe-submission-time	m	m	m	m		
2.3	content-identifier	o	c1	m	m		

c1 - if supported in probe submission envelope then m else –

A.1.3.4 CancelDeferredDelivery

Ref	Element	UA		MS		Support	Notes/References
		Base	Profile	Base	Profile		
1	ARGUMENT						
1.1	message-submission-identifier	m	m	m	m		see A.1.8/8
2	RESULT						
2.1	NULL	m	m	m	m		

A.1.3.5 SubmissionControl

Ref	Element	UA		MS		Support	Notes/References
		Base	Profile	Base	Profile		
1	ARGUMENT						
1.1	controls	m	m	m	m		
1.1.1	restrict	m	m	o	m		
1.1.2	permissible-operations	m	m	o	c1		
1.1.3	permissible-maximum-content-length	m	m	o	c1		
1.1.4	permissible-lowest-priority	m	m	o	c1		
1.1.5	permissible-security-context	o	o	o	o		see A.1.9/3
2	RESULT						
2.1	waiting	m	m	m	m		
2.1.1	waiting-operations	o	o	m	m		
2.1.2	waiting-messages	o	o	m	m		
2.1.3	waiting-content-types	o	o	m	m		
2.1.4	waiting-encoded-information-types	o	o	m	m		see A.1.8/10

c1 - if the MS has a P3 interface to the MTA then m else if supported by the MTA then m else o

A.1.3.6 Summarize

Ref	Element	UA		MS		Support	Notes/References
		Base	Profile	Base	Profile		
1	ARGUMENT						
1.1	information-base-type	o	o	m	m		see A.1.8/5
1.2	selector	m	m	m	m		see A.1.8/7
1.3	summary-requests	o	o	m	m		
2	RESULT						
2.1	next	m	m	m	m		
2.2	count	m	m	m	m		
2.3	span	m	m	m	m		
2.4	summaries	o	c1	m	m		
2.4.1	absent	m	m	m	m		
2.4.2	present	m	m	m	m		
2.4.2.1	type	m	m	m	m		
2.4.2.2	value	m	m	m	m		
2.4.2.3	count	m	m	m	m		

c1 - if the request is supported then m else –

A.1.3.7 List

Ref	Element	UA		MS		Support	Notes/References
		Base	Profile	Base	Profile		
1	ARGUMENT						
1.1	information-base-type	o	o	m	m		see A.1.8/5
1.2	selector	m	m	m	m		see A.1.8/7
1.3	requested-attributes	m	m	m	m		see A.1.8/1
2	RESULT						
2.1	next	m	m	m	m		
2.2	requested	m	m	m	m		see A.1.8/2

A.1.3.8 Fetch

Ref	Element	UA		MS		Support	Notes/References
		Base	Profile	Base	Profile		
1	ARGUMENT						
1.1	information-base-type	o	o	m	m		see A.1.8/5
1.2	item	m	m	m	m		
1.2.1	search	o	o	o	m		see A.1.8/7
1.2.2	precise	o	o	o	m		
1.3	requested-attributes	m	m	m	m		see A.1.8/1
2	RESULT						
2.1	entry-information	m	m	m	m		see A.1.8/2
2.2	list	o	o	o	m		
2.3	next	o	o	o	m		

A.1.3.9 Delete

Ref	Element	UA		MS		Support	Notes/References
		Base	Profile	Base	Profile		
1	ARGUMENT						
1.1	information-base-type	o	o	m	m		see A.1.8/5
1.2	items	m	m	m	m		

1.2.1	selector	o	o	m	m		see A.1.8/7
1.2.2	sequence-numbers	o	m	m	m		
2	RESULT						
2.1	NULL	m	m	m	m		

A.1.3.10 Register-MS

Ref	Element	UA		MS		Support	Notes/References
		Base	Profile	Base	Profile		
1	ARGUMENT						
1.1	auto-action-registrations	o	o	o	o		
1.1.1	auto-forward	o	o	o	o		see A.1.6
1.1.2	auto-alert	o	o	o	o		see A.1.7
1.2	auto-action-deregistrations	o	o	o	o		
1.2.1	auto-forward	o	o	o	o		
1.2.2	auto-alert	o	o	o	o		
1.3	list-attribute-defaults	o	o	o	o		
1.4	fetch-attribute-defaults	o	o	o	o		
1.5	change-credentials	m	m	m	m		
1.5.1	old-credentials	m	m	m	m		
1.5.1.1	simple	m	m	m	m		
1.5.1.1.1	IA5 String	o	o	m	m		
1.5.1.1.2	OCTET STRING	o	m	m	m		
1.5.1.2	strong	o	o	o	o		
1.5.1.2.1	bind-token	m	m	m	m		see A.1.3.1
1.5.1.2.2	certificate	o	o	o	o		
1.5.2	new-credentials	m	m	m	m		
1.5.2.1	simple	m	m	m	m		
1.5.2.1.1	IA5 String	o	o	m	m		
1.5.2.1.2	OCTET STRING	o	m	m	m		
1.5.2.2	strong	o	o	o	o		
1.5.2.2.1	bind-token	m	m	m	m		see A.1.3.1
1.5.2.2.2	certificate	o	o	o	o		
1.6	user-security-labels	o	o	o	o		see A.1.9/3

2	RESULT						
2.1	NULL	m	m	m	m		

A.1.3.11 Alert

Ref	Element	UA		MS		Support	Notes/References
		Base	Profile	Base	Profile		
1	ARGUMENT						
1.1	alert-registration-identifier	m	m	m	m		
1.2	new-entry	o	o	m	m		see A.1.8/2
2	RESULT						
2.1	NULL	m	m	m	m		

A.1.3.12 Register

Ref	Element	UA		MS		Support	Notes/References
		Base	Profile	Base	Profile		
1	ARGUMENT						
1.1	user-name	o	o	o	c1		see A.1.10
1.2	user-address	o	o	o	c1		
1.3	deliverable-encoded-information-types	o	o	o	c1		see A.1.8/10
1.4	deliverable-maximum-content-length	o	o	o	c1		
1.5	default-delivery-controls	o	o	o	c1		
1.5.1	restrict	o	o	o	c1		
1.5.2	permissible-operations	o	o	o	c1		
1.5.3	permissible-maximum-content-length	o	o	o	c1		
1.5.4	permissible-lowest-priority	o	o	o	c1		
1.5.5	permissible-content-types	o	o	o	c1		
1.5.6	permissible-encoded-information-types	o	o	o	c1		see A.1.8/10
1.6	deliverable-content-types	o	o	o	c1		
1.7	labels-and-redirections	o	o	o	c1		
1.7.1	user-security-label	o	o	o	c1		see A.1.9/3

1.7.2	recipient-assigned-alternate-recipient	o	o	o	c1		
2	RESULT						
2.1	NULL	m	m	m	m		

c1 - if the MS has a P3 interface to the MTA then m else if supported by the MTA then m else o

A.1.3.13 ChangeCredentials

Ref	Element	UA		MS		Support	Notes/References
		Base	Profile	Base	Profile		
1	ARGUMENT						
1.1	old-credentials	m	m	m	m		
1.1.1	simple	m	m	m	m		
1.1.1.1	IA5String	o	o	m	m		
1.1.1.2	OCTET STRING	o	m	m	m		
1.1.2	strong	o	o	o	c1		
1.1.2.1	bind-token	m	m	m	m		see A.1.3.1
1.1.2.2	certificate	o	o	o	c1		
1.2	new-credentials	m	m	m	m		
1.2.1	simple	m	m	m	m		
1.2.1.1	IA5String	o	o	m	m		
1.2.1.2	OCTET STRING	o	m	m	m		
1.2.2	strong	o	o	o	c1		
1.2.2.1	bind-token	m	m	m	m		see A.1.3.1
1.2.2.2	certificate	o	o	o	c1		
2	RESULT						
2.1	NULL	m	m	m	m		

c1 - if the MS has a P3 interface to the MTA then m else if supported by the MTA then m else o

A.1.4 MessageSubmissionEnvelope

Ref	Element	UA		MS		Support	Notes/References
		Base	Profile	Base	Profile		
1	originator-name	m	m	m	m		see A.1.10
2	original-encoded-information-types	m	m	m	m		see A.1.8/10
3	content-type	m	m	m	m		see A.1.8/11
4	content-identifier	o	o	m	m		
5	priority	m	m	m	m		
6	per-message-indicators	m	m	m	m		see A.1.8/12
7	deferred-delivery-time	o	o	m	m		
8	extensions						
8.1	recipient-reassignment-prohibited	o	m2	o	m		
8.2	dl-expansion-prohibited	o	m2	o	m		
8.3	conversion-with-loss-prohibited	o	o	o	m		
8.4	latest-delivery-time	o	o	o	c1		
8.5	originator-return-address	o	o	o	c1		see A.1.10
8.6	originator-certificate	o	o	o	c1		
8.7	content-confidentiality-algorithm-identifier	o	o	o	c1		
8.8	message-origin-authentication-check	o	o	o	c1		see A.1.9/2
8.9	message-security-label	o	o	o	c1		see A.1.9/3
8.10	proof-of-submission-request	o	i	o	i		
8.11	content-correlator	o	o	m	m		
8.12	forwarding-request	o	o	o	o		
9	per-recipient-fields	m	m	m	m		
9.1	recipient-name	m	m	m	m		see A.1.10
9.2	originator-report-request	m	m	m	m		
9.3	explicit-conversion	o	o	o	m		
9.4	extensions						

9.4.1	originator-requested-alternate-recipient	o	o	o	c1		see A.1.10
9.4.2	requested-delivery-method	o	o	o	c1		
9.4.3	physical-forwarding-prohibited	o	o	o	c1		
9.4.4	physical-forwarding-address-request	o	o	o	c1		
9.4.5	physical-delivery-modes	o	o	o	c1		
9.4.6	registered-mail-type	o	o	o	c1		
9.4.7	recipient-number-for-advice	o	o	o	c1		
9.4.8	physical-rendition-attributes	o	o	o	c1		
9.4.9	physical-delivery-report-request	o	o	o	c1		
9.4.10	message-token	o	o	o	c1		see A.1.9/4
9.4.11	content-integrity-check	o	o	o	c1		
9.4.12	proof-of-delivery-request	o	o	o	c1		

c1 - if the MS has a P3 interface to the MTA then m else if supported by the MTA then m else o

m2 - only the capability to generate the "prohibited" value is required

A.1.5 ProbeSubmissionEnvelope

Ref	Element	UA		MS		Support	Notes/References
		Base	Profile	Base	Profile		
1	originator-name	m	m	m	m		see A.1.10
2	original-encoded-information-types	m	m	m	m		see A.1.8/10
3	content-type	m	m	m	m		see A.1.8/11
4	content-identifier	o	o	m	m		
5	content-length	o	m	m	m		
6	per-message-indicators	m	m	m	m		see A.1.8/12
7	extensions						
7.1	recipient-reassignment-prohibited	o	m2	o	m		
7.2	dl-expansion-prohibited	o	m2	o	m		
7.3	conversion-with-loss-prohibited	o	o	o	m		
7.4	originator-certificate	o	o	o	c1		
7.5	message-security-label	o	o	o	c1		see A.1.9/3
7.6	content-correlator	o	o	m	m		
7.7	probe-origin-authentication-check	o	o	o	c1		see A.1.9/5
8	per-recipient-fields	m	m	m	m		
8.1	recipient-name	m	m	m	m		see A.1.10
8.2	originator-report-request	m	m	m	m		
8.3	explicit-conversion	o	o	o	m		
8.4	extensions						
8.4.1	originator-requested-alternate-recipient	o	o	o	c1		see A.1.10
8.4.2	requested-delivery-method	o	o	o	c1		
8.4.3	physical-rendition-attributes	o	o	o	c1		

c1 - if the MS has a P3 interface to the MTA then m else if supported by the MTA then m else o

m2 - only the capability to generate the "prohibited" value is required

A.1.6 AutoForwardRegistrationParameter

Ref	Element	UA		MS		Support	Notes/References
		Base	Profile	Base	Profile		
1	filter	o	o	m	m		see A.1.8/3
2	auto-forward-arguments	m	m	m	m		
2.1	originator-name	m	m	m	m		see A.1.10
2.2	content-identifier	o	c1	o	m		
2.3	priority	o	o	o	m		
2.4	per-message-indicators	o	m	m	m		see A.1.8/12
2.5	deferred-delivery-time	o	o	o	m		
2.6	extensions	o	c2	o	m		see A.1.4/8
2.7	per-recipient-fields	o	c2	m	m		see A.1.4/9
3	delete-after-auto-forwarding	o	o	m	m		
4	other-parameters	o	o	o	o		

c1 - if supported in message submission envelope then m else o

c2 - the requirements for support of the sub-elements of this element are as specified in ISO/IEC ISP 10611-4 (i.e., a claim of support of this element means that at least the minimum requirements of ISO/IEC ISP 10611-4 with respect to the component sub-elements are met)

A.1.7 AutoAlertRegistrationParameter

Ref	Element	UA		MS		Support	Notes/References
		Base	Profile	Base	Profile		
1	filter	o	o	m	m		see A.1.8/3
2	alert-addresses	o	o	o	o		
2.1	address	m	m	m	m		
2.2	alert-qualifier	o	o	o	o		
3	requested-attributes	o	o	m	m		see A.1.8/1

A.1.8 Common data types

Ref	Element	UA		MS		Support	Notes/References
		Base	Profile	Base	Profile		
1	AttributeSelection						
1.1	type	m	m	m	m		
1.2	from	o	o	o	m		
1.3	count	o	o	o	m		
2	EntryInformation						
2.1	sequence-number	m	m	m	m		
2.2	attributes	m	m	m	m		
3	Filter						
3.1	item	m	m	m	m		see A.1.8/4
3.2	and	o	o	m	m		
3.3	or	o	o	m	m		
3.4	not	o	m	m	m		
4	FilterItem						
4.1	equality	o	o	m	m		
4.2	substrings	o	o	o	o		
4.2.1	type	m	m	m	m		
4.2.2	strings	m	m	m	m		
4.2.2.1	initial	o	o	m	m		
4.2.2.2	any	o	o	m	m		
4.2.2.3	final	o	o	m	m		
4.3	greater-or-equal	o	o	m	m		
4.4	less-or-equal	o	o	m	m		
4.5	present	o	o	m	m		
4.6	approximate-match	o	o	o	o		
5	InformationBase						

5.1	stored-messages	m	m	m	m		
5.2	inlog	–	i	–	i		
5.3	outlog	–	i	–	i		
6	Range						
6.1	sequence-number-range	o	o	m	m		
6.1.1	from	o	o	m	m		
6.1.2	to	o	o	m	m		
6.2	creation-time-range	o	o	m	m		
6.2.1	from	o	o	m	m		
6.2.2	to	o	o	m	m		
7	Selector						
7.1	child-entries	o	o	m	m		
7.2	range	o	o	m	m		see A.1.8/6
7.3	filter	o	o	m	m		see A.1.8/3
7.4	limit	o	m	m	m		
7.5	override	o	c1	o	c1		
8	MTSIdentifier						
8.1	global-domain-identifier	m	m	m	m		see A.1.8/9
8.2	local-identifier	m	m	m	m		
9	GlobalDomainIdentifier						
9.1	country-name	m	m	m	m		
9.2	administration-domain-name	m	m	m	m		
9.3	private-domain-identifier	o	m	o	m		
10	EncodedInformationTypes						
10.1	built-in-encoded-information-types	m	m	m	m		
10.2	(non-basic parameters)	o	o	o	c2		
10.3	extended-encoded-information-types	o	m	o	m		

11	ContentType						
11.1	built-in	o	o	o	m		
11.2	extended	o	o	o	m		
12	PerMessageIndicators						
12.1	disclosure-of-other-recipients	o	o	m	m		
12.2	implicit-conversion-prohibited	m	m	m	m		
12.3	alternate-recipient-allowed	o	o	m	m		
12.4	content-return-request	o	o	o	c2		
12.5	reserved	o	o	o	m		in CCITT X.411 only
12.6	bit-5	o	o	o	m		in CCITT X.411 only
12.7	bit-6	o	o	o	m		in CCITT X.411 only
12.8	service-message	o	o	o	m		in CCITT X.411 only

c1 - if fetch restrictions are supported then m else –

c2 - if the MS has a P3 interface to the MTA then m else if supported by the MTA then m else o

A.1.9 Extension data types

Ref	Element	UA		MS		Support	Notes/References
		Base	Profile	Base	Profile		
1	ExtensionField						
1.1	type	o	m	m	m		
1.1.1	standard-extension	m	m	m	m		
1.1.2	private-extension	o	o	m	m		not in CCITT X.411
1.2	criticality	m	m	m	m		
1.3	value	m	m	m	m		
2	MessageOriginAuthenticationCheck						
2.1	algorithm-identifier	m	m	m	m		
2.2	content	m	m	m	m		
2.3	content-identifier	o	m	o	m		
2.4	message-security-label	o	m	o	m		see A.1.9/3
3	MessageSecurityLabel						
3.1	security-policy-identifier	o	o	o	m		
3.2	security-classification	o	o	o	m		
3.3	privacy-mark	o	o	o	m		
3.4	security-categories	o	o	o	m		
4	MessageToken						
4.1	token-type-identifier	m	m	m	m		
4.2	asymmetric-token	m	m	m	m		
4.2.1	signature-algorithm-identifier	m	m	m	m		
4.2.2	name	m	m	m	m		
4.2.3	time	m	m	m	m		
4.2.4	signed-data	o	o	o	m		
4.2.4.1	content-confidentiality-algorithm-identifier	o	o	o	m		

4.2.4.2	content-integrity-check	o	o	o	m		
4.2.4.3	message-security-label	o	o	o	m		see A.1.9/3
4.2.4.4	proof-of-delivery-request	o	o	o	m		
4.2.4.5	message-sequence-number	o	o	o	m		
4.2.5	encryption-algorithm-identifier	o	o	o	m		
4.2.6	encrypted-data	o	o	o	m		
4.2.6.1	content-confidentiality-key	o	o	o	m		
4.2.6.2	content-integrity-check	o	o	o	m		
4.2.6.3	message-security-label	o	o	o	m		see A.1.9/3
4.2.6.4	content-integrity-key	o	o	o	m		
4.2.6.5	message-sequence-number	o	o	o	m		
5	ProbeOriginAuthenticationCheck						
5.1	algorithm-identifier	m	m	m	m		
5.2	content-identifier	o	m	o	m		
5.3	message-security-label	o	m	o	m		see A.1.9/3
6	ProofOfSubmission						
6.1	algorithm-identifier	m	m	m	m		
6.2	message-submission-envelope	m	m	m	m		
6.3	content	m	m	m	m		
6.4	message-submission-identifier	m	m	m	m		
6.5	message-submission-time	m	m	m	m		

A.1.10 O/R names

Ref	O/R Name Form	UA		MS		Support	Notes/References
		Base	Profile	Base	Profile		
1	mnemonic O/R address	m	m	m	m		see A.1.10.1
2	numeric O/R address	o	o	m	m		see A.1.10.2
3	terminal O/R address	o	o	m	m		see A.1.10.3
4	formatted postal O/R address	o	o	m	m		see A.1.10.4
5	unformatted postal O/R address	o	o	m	m		see A.1.10.5
6	directory-name	o	o	m	m		

A.1.10.1 Mnemonic O/R address

Ref	Element	UA		MS		Support	Notes/References
		Base	Profile	Base	Profile		
1	built-in-standard-attributes	m	m	m	m		
1.1	country-name	m	m	m	m		
1.2	administration-domain-name	m	m	m	m		
1.3	private-domain-name	o	m	m	m		
1.4	organization-name	o	m	m	m		
1.5	personal-name	o	m	m	m		
1.5.1	surname	m	m	m	m		
1.5.2	given-name	o	m	m	m		
1.5.3	initials	o	m	m	m		
1.5.4	generation-qualifier	o	m	m	m		
1.6	organizational-unit-names	o	m	m	m		
2	built-in-domain-defined-attributes	o	m	m	m		
3	extension-attributes	o	m	m	m		
3.1	common-name	o	m	m	m		
3.2	teletex-common-name	o	m	m	m		
3.3	teletex-organization-name	o	m	m	m		
3.4	teletex-personal-name	o	m	m	m		

3.4.1	surname	m	m	m	m		
3.4.2	given-name	o	m	m	m		
3.4.3	initials	o	m	m	m		
3.4.4	generation-qualifier	o	m	m	m		
3.5	teletex-organizational-unit-names	o	m	m	m		
3.6	teletex-domain-defined-attributes	o	m	m	m		

A.1.10.2 Numeric O/R address

Ref	Element	UA		MS		Support	Notes/References
		Base	Profile	Base	Profile		
1	built-in-standard-attributes	m	m	m	m		
1.1	country-name	m	m	m	m		
1.2	administration-domain-name	m	m	m	m		
1.3	private-domain-name	o	m	m	m		
1.4	numeric-user-identifier	m	m	m	m		
2	built-in-domain-defined-attributes	o	m	m	m		
3	extension-attributes	o	m	m	m		
3.1	teletex-domain-defined-attributes	o	m	m	m		

A.1.10.3 Terminal O/R address

Ref	Element	UA		MS		Support	Notes/References
		Base	Profile	Base	Profile		
1	built-in-standard-attributes	m	m	m	m		
1.1	country-name	o	m	m	m		
1.2	administration-domain-name	o	m	m	m		
1.3	network-address	m	m	m	m		
1.4	terminal-identifier	o	m	m	m		
1.5	private-domain-name	o	m	m	m		
2	built-in-domain-defined-attributes	o	m	m	m		
3	extension-attributes	o	m	m	m		
3.1	extended-network-address	m	m	m	m		
3.1.1	e163-4-address	o	o	m	m		
3.1.2	psap-address	o	o	m	m		
3.2	terminal-type	o	m	m	m		
3.3	teletex-domain-defined-attributes	o	m	m	m		

A.1.10.4 Formatted postal O/R address

Ref	Element	UA		MS		Support	Notes/References
		Base	Profile	Base	Profile		
1	built-in-standard-attributes	m	m	m	m		
1.1	country-name	m	m	m	m		
1.2	administration-domain-name	m	m	m	m		
1.3	private-domain-name	o	m	m	m		
2	extension-attributes	m	m	m	m		
2.1	physical-delivery-country-name	m	m	m	m		
2.2	physical-delivery-office-name	o	m	m	m		
2.3	physical-delivery-office-number	o	m	m	m		
2.4	physical-delivery-organization-name	o	m	m	m		
2.5	physical-delivery-personal-name	o	m	m	m		
2.6	postal-code	m	m	m	m		
2.7	poste-restante-address	o	m	m	m		
2.8	post-office-box-address	o	m	m	m		
2.9	pds-name	o	m	m	m		
2.10	street-address	o	m	m	m		
2.11	unique-postal-name	o	m	m	m		
2.12	extension-OR-address-components	o	m	m	m		
2.13	extension-physical-delivery-address-components	o	m	m	m		
2.14	local-postal-attributes	o	m	m	m		

A.1.10.5 Unformatted postal O/R address

Ref	Element	UA		MS		Support	Notes/References
		Base	Profile	Base	Profile		
1	built-in-standard-attributes	m	m	m	m		
1.1	country-name	m	m	m	m		
1.2	administration-domain-name	m	m	m	m		
1.3	private-domain-name	o	m	m	m		
2	extension-attributes	m	m	m	m		
2.1	unformatted-postal-address	m	m	m	m		
2.2	physical-delivery-country-name	m	m	m	m		
2.3	postal-code	m	m	m	m		
2.4	pds-name	o	m	m	m		

A.1.11 General attributes

Ref	Attribute	UA		MS		Support	Notes/References
		Base	Profile	Base	Profile		
1	child-sequence-numbers	m	m	m	m		
2	content	m	m	m	m		
3	content-confidentiality-algorithm-identifier	o	o	o	o		
4	content-correlator	o	o	o	o		
5	content-identifier	o	o	o	o		
6	content-integrity-check	o	o	o	o		
7	content-length	o	o	o	m		
8	content-returned	o	o	o	o		
9	content-type	m	m	m	m		
10	conversion-with-loss-prohibited	o	o	o	o		
11	converted-eits	o	o	o	o		
12	creation-time	m	m	m	m		
13	delivered-eits	o	o	o	m		

14	delivery-flags	o	o	o	o		
15	dl-expansion-history	o	o	o	o		
16	entry-status	m	m	m	m		
17	entry-type	m	m	m	m		
18	intended-recipient-name	o	o	o	o		
19	message-delivery-envelope	m	m1	m	m		
20	message-delivery-identifier	o	o	o	o		
21	message-delivery-time	o	o	o	o		
22	message-origin-authentication-check	o	o	o	o		
23	message-security-label	o	o	o	o		
24	message-submission-time	o	o	o	o		
25	message-token	o	o	o	o		
26	original-eits	o	o	o	o		
27	originator-certificate	o	o	o	o		
28	originator-name	o	o	o	o		
29	other-recipient-names	o	o	o	o		
30	parent-sequence-number	m	m	m	m		
31	per-recipient-report-delivery-fields	m	m	m	m		
32	priority	o	o	o	m		
33	proof-of-delivery-request	o	o	o	o		
34	redirection-history	o	o	o	o		
35	report-delivery-envelope	m	m1	m	m		
36	reporting-dl-name	o	o	o	o		
37	reporting-mta-certificate	o	o	o	o		
38	report-origin-authentication-check	o	o	o	o		
39	security-classification	o	o	o	o		
40	sequence-number	m	m	m	m		
41	subject-submission-identifier	m	m	m	m		
42	this-recipient-name	o	o	o	o		

m1 - the requirements for support of the elements of a delivery envelope by a UA are as specified in ISO/IEC ISP 10611-4 (i.e., a claim of support of such an attribute means that at least the minimum requirements of ISO/IEC ISP 10611-4 with respect to the component elements of the envelope are met)

A.2 Optional functional groups

The following requirements are additional to those specified in A.1 if support of the functional group is claimed.

A.2.1 Security (SEC)

The support requirements for all SEC classes are as specified in A.1 unless otherwise specified below. Elements classified as cC shall be treated as m if support of a confidential security class variant (SnC) is claimed, else as o.

A.2.1.1 Operation arguments/results

A.2.1.1.1 MS-bind

Ref	Element	UA			MS		
		S0	S1	S2	S0	S1	S2
1.2	initiator-credentials						
1.2.1	simple		ix	ix		ix	ix
1.2.2	strong		mr	mr		mr	mr
1.2.2.1.4	signed-data		mr	mr		mr	mr
1.3	security-context		mr	mr		mr	mr
2.1	responder-credentials						
2.1.1	simple		ix	ix		ix	ix
2.1.2	strong		mr	mr		mr	mr
2.1.2.1.4	signed-data		mr	mr		mr	mr

A.2.1.1.2 MessageSubmission

Ref	Element	UA			MS		
		S0	S1	S2	S0	S1	S2
2.4.1	originating-MTA-certificate	ix	ix	o	ix	ix	o
2.4.2	proof-of-submission	ix	ix	m	ix	ix	m

A.2.1.1.3 SubmissionControl

Ref	Element	UA			MS		
		S0	S1	S2	S0	S1	S2
1.1.2	permissible-operations				m	m	m
1.1.3	permissible-maximum-content-length				m	m	m
1.1.4	permissible-lowest-priority				m	m	m
1.1.5	permissible-security-context		m	m		m	m

A.2.1.1.5 Register-MS

Ref	Element	UA			MS		
		S0	S1	S2	S0	S1	S2
1.5	change-credentials						
1.5.1	old-credentials						
1.5.1.1	simple		ix	ix		ix	ix
1.5.1.2	strong		m	m		m	m
1.5.2	new-credentials						
1.5.2.1	simple		ix	ix		ix	ix
1.5.2.2	strong		m	m		m	m
1.6	user-security-labels		m	m		m	m

A.2.1.1.6 Register

Ref	Element	UA			MS		
		S0	S1	S2	S0	S1	S2
1.1	user-name		m	m		m	m
1.7.1	user-security-label		m	m		m	m

A.2.1.1.7 ChangeCredentials

Ref	Element	UA			MS		
		S0	S1	S2	S0	S1	S2
1.1.1	simple		ix	ix		ix	ix
1.1.2	strong		m	m		m	m
1.2.1	simple		ix	ix		ix	ix
1.2.2	strong		m	m		m	m

A.2.1.2 MessageSubmissionEnvelope

Ref	Element	UA			MS		
		S0	S1	S2	S0	S1	S2
8.6	originator-certificate				m	m	m
8.7	content-confidentiality-algorithm-identifier	cC	cC	cC	m	m	m
8.8	message-origin-authentication-check			mr	m	m	mr
8.9	message-security-label		mr	mr	m	mr	mr
8.10	proof-of-submission-request			m			m
9.4.10	message-token	m	mr	mr	m	mr	mr
9.4.11	content-integrity-check	m	m	m	m	m	m
9.4.12	proof-of-delivery-request	m	m	m	m	m	m

A.2.1.3 ProbeSubmissionEnvelope

Ref	**Element**	**UA**			**MS**		
		S0	**S1**	**S2**	**S0**	**S1**	**S2**
7.4	originator-certificate				m	m	m
7.5	message-security-label		mr	mr	m	mr	mr
7.7	probe-origin-authentication-check			mr	m	m	mr

A.2.1.4 Extension data types

Ref	Element	UA			MS		
		S0	S1	S2	S0	S1	S2
2	MessageOriginAuthenticationCheck						
2.4	message-security-label		mr	mr		mr	mr
3	MessageSecurityLabel						
3.1	security-policy-identifier		mr	mr		mr	mr
3.2	security-classification		m	m		m	m
3.3	security-categories		m	m		m	m
4	MessageToken						
4.2.4	signed-data	m	m	m	m	m	m
4.2.4.1	content-confidentiality-algorithm-identifier	cC	cC	cC	m	m	m
4.2.4.2	content-integrity-check	m	m	m	m	m	m
4.2.4.3	message-security-label		m	m		m	m
4.2.4.4	proof-of-delivery-request	m	m	m	m	m	m
4.2.5	encryption-algorithm-identifier		m	m		m	m
4.2.6	encrypted-data		m	m		m	m
4.2.6.2	content-integrity-check	m	m	m	m	m	m
4.2.6.3	message-security-label		m	m		m	m
5	ProbeOriginAuthenticationCheck						
5.3	message-security-label		mr	mr		mr	mr

A.2.1.5 General attributes

Ref	Element	UA			MS		
		S0	S1	S2	S0	S1	S2
3	content-confidentiality-algorithm-identifier	cC	cC	cC	cC	cC	cC

6	content-integrity-check	m	m	m	m	m	m
22	message-origin-authentication-check			m			m
23	message-security-label		m	m		m	m
25	message-token	m	m	m	m	m	m
33	proof-of-delivery-request	m	m	m	m	m	m
38	report-origin-authentication-check			m			m
39	security-classification		m	m		m	m

A.2.2 Physical Delivery (PD)

The support requirements specified below are for a UA and for an MS on submission. Support of the PDAU is specified in ISO/IEC ISP 10611-3 and ISO/IEC ISP 10611-4.

A.2.2.1 MessageSubmissionEnvelope

Ref	Element	Profile	
		UA	MS
8.5	originator-return-address		m
9.4.3	physical-forwarding-prohibited	m	m
9.4.4	physical-forwarding-address-request		m
9.4.5	physical-delivery-modes	m	m
9.4.6	registered-mail-type		m
9.4.7	recipient-number-for-advice		m
9.4.8	physical-rendition-attributes		m
9.4.9	physical-delivery-report-request		m

A.2.2.2 ProbeSubmissionEnvelope

Ref	Element	Profile	
		UA	MS
8.4.3	physical-rendition-attributes		m

A.2.2.3 O/R names

Ref	O/R Name Form	Profile	
		UA	MS
4	formatted postal O/R address	m	
5	unformatted postal O/R address	m	

A.2.3 Latest Delivery (LD)

A.2.3.1 MessageSubmissionEnvelope

Ref	Element	Profile	
		UA	MS
8.4	latest-delivery-time	m	

A.2.4 Return of Content (RoC)

A.2.4.1 Common data types

Ref	Element	Profile	
		UA	MS
12	PerMessageIndicators		
12.4	content-return-request	m	

A.2.5 Use of Directory (DIR)

A.2.5.1 O/R names

Ref	O/R name Form	Profile	
		UA	MS
6	directory-name	m	

A.3 Additional information

A.3.1 Content types supported

The following table shall be completed to indicate (Y or 3) which content type(s) the implementation can support on submission and on retrieval (see clause 6 of ISO/IEC ISP 10611-1).

Ref	Content Type	Supported		Comments
		Submission	Retrieval	
1	built-in			
1.1	unidentified (0)			
1.2	interpersonal-messaging-1984 (2)			
1.3	interpersonal-messaging-1988 (22)			
1.4	(EDI messaging) (35)			
2	extended (specify)			

A.3.2 Encoded information types supported

The following table shall be completed to indicate (Y or 3) which encoded information type(s) the implementation can support on submission and on retrieval (see clause 6 of ISO/IEC ISP 10611-1).

Ref	Encoded Information Type	Supported		Comments
		Submission	Retrieval	
1	built-in			
1.1	undefined (0)			
1.2	ia5-text (2)			
1.3	g3-facsimile (3)			
1.4	g4-class-1 (4)			
1.5	teletex (5)			
1.6	videotex (6)			
1.7	voice (7)			
1.8	mixed-mode (9)			
1.9	other (specify)			
2	extended (specify)			

A.3.3 Support of filter

The following table shall be completed to indicate any constraints on the support of filter.

Ref	Constraint	Value	Comments
1	Maximum number of levels of recursion/nesting of filter supported		

2	Maximum number of elements that can be logically combined at any one level		

Annex B

(normative)

Amendments and corrigenda

International Standards are subject to constant review and revision by the ISO/IEC Technical Committees concerned. The following amendments and corrigenda are approved by ISO/IEC JTC1 and are considered as normative references in this part of ISO/IEC ISP 10611.

NOTE - Corresponding corrigenda to the equivalent CCITT Recommendations are contained in the joint CCITT/ISO MHS Implementor's Guide.

MOTIS

ISO/IEC 10021-1/Cor.1:1991

ISO/IEC 10021-1/Cor.2:1991

ISO/IEC 10021-1/Cor.3:1992

ISO/IEC 10021-1/Cor.4:1992

ISO/IEC 10021-1/Cor.5:1992

ISO/IEC 10021-2/Cor.1:1991

ISO/IEC 10021-2/Cor.2:1991

ISO/IEC 10021-2/Cor.3:1992

ISO/IEC 10021-2/Cor.4:1992

ISO/IEC 10021-4/Cor.1:1991

ISO/IEC 10021-4/Cor.2:1991

ISO/IEC 10021-4/Cor.3:1992

ISO/IEC 10021-4/Cor.4:1992

ISO/IEC 10021-4/Cor.5:1992

ISO/IEC 10021-5/Cor.1:1991

ISO/IEC 10021-5/Cor.2:1991

ISO/IEC 10021-5/Cor.3:1992

ISO/IEC 10021-5/Cor.4:1992

ISO/IEC 10021-6/Cor.1:1991

ISO/IEC 10021-6/Cor.2:1991

ISO/IEC 10021-6/Cor.3:1992

ISO/IEC 10021-6/Cor.4:1992

ISO/IEC 10021-6/Cor.5:1992

ISO/IEC 10021-5/Cor.5:1992

To: P Bessems (ISO/IEC JTC1/SGFS Secretariat)

cc: EWOS Secretariat
MHS ISP Special Group (MISG)

From: Jon Stranger (Editor, AMH1 ISPs)

Date: 14th August 1993

Subject: Editorial Errata - ISO/IEC DISP 10611 (AMH1)

This document identifies a number of errata to pDISP 10611 which have come to light since submission to ISO/IEC JTC1/SGFS and which have been corrected by the editor in the preparation of the DISP texts. All changes are considered editorial in nature.

ISO/IEC DISP 10611-n (all parts)

Contents page Insert ‘Unless otherwise specified' at the beginning of the 2nd sentence of the copyright notice (alignment with latest JTC1 standard text).

ISO/IEC DISP 10611-1

7.7.2 The reference to table 2 in the 1st sentence of the 2nd paragraph should be to table 3 (editorial error).

C.3.5.6 Change the reference in the 2nd paragraph to ‘UK-Netherlands-Germany-France draft IT Security Evaluation Criteria' to ‘European Information Technology Security Evaluation Criteria [ITSEC]' (update to external reference).

Insert a right parenthesis after ‘comparison' in the 3rd paragraph (editorial error).

ISO/IEC DISP 10611-2

cover page Change reference to the CULR ISP to ‘Working Draft Version 14' (update to external reference).

A.3.2 Renumber the second instance of A.3.2 (and subclauses) as A.3.3 (editorial error).

A.4.1 Remove clause A.4.1 (made redundant by latest revision of the CULR ISP).

ISO/IEC DISP 10611-3

A.2 Remove the Support column from all tables in A.2 (since A.2 is effectively an IPRL of the PICS proforma in A.1).

ISO/IEC DISP 10611-4

A.2 Remove the Support column from all tables in A.2 (since A.2 is effectively an IPRL of the PICS proforma in A.1).

ISO/IEC DISP 10611-5

3.2.1 Add the following clarification to the definition of mandatory support (m): ‘Mandatory support of an MS attribute means that it is supported in the context of all applicable supported operation arguments and results and also for use within a selector to the level of support claimed for the filter item.' (editorial clarification).

5.1 Replace ‘supports MS or MS-user functionality' by ‘claims conformance as an MS or as an MS-user' (editorial improvement).

A.2 Remove the Support column from all tables in A.2 (since A.2 is effectively an IPRL of the PICS proforma in A.1).

A.3.1 Amend the preamble to the table to refer to ‘retrieval' rather than ‘delivery'. Remove the 2nd sentence of the preamble and amend the table to include separate columns for submission and retrieval (editorial error).

A.3.2 Amend the preamble to the table to refer to ‘retrieval' rather than ‘delivery'. Amend the table to include separate columns for submission and retrieval (editorial error).

To: P Bessems (ISO/IEC JTC1/SGFS Secretariat)

cc: EWOS Secretariat
MHS ISP Special Group (MISG)

From: Jon Stranger (Editor, AMH1 ISPs)

Date: 14th August 1993

Subject: Editor's Comments on ISO/IEC DISP 10611-5 (AMH13)

This document identifies some proposed changes to ISO/IEC DISP 10611-5 which have come to light since submission to ISO/IEC JTC1/SGFS for reasons of alignment with the proposed text for part 5 of the AMH2 ISP. National bodies are requested to take these proposals into consideration when preparing their ballot comments.

clause

A.1.11 Change the MS support for the originator-name attribute (A.1.11/28) to m and add a note 'A change to the base standards has been proposed to require support of this attribute.'

A.3.1 Revise the scope of this clause to allow support of MS attributes also to be claimed if support of the content type on retrieval is claimed. A claim of support of MS attributes in this context will mean that any mandatory requirements in the relevant content type-specific base standards for support of MS attributes are met.

Add a 2nd paragraph to the preamble: 'If support on retrieval is claimed, then support of MS attributes may also be claimed. A claim of support of attributes means that any mandatory requirements in the relevant content type-specific base standards for support of MS attributes are met.'

Amend the table to add an Attributes column. Mark the Attributes column as not applicable for unidentified and ipm-1984. Add a note against ipm-1988: 'A change to the IPM base standards has been proposed to require support of the subject attribute. It is strongly recommended that this attribute is supported.'