INTERNATIONAL STANDARDIZED PROFILE

ISO/IEC ISP 10611-1

First edition
1994-10-15

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

Part 1:
MHS Service Support

Technologies de l'information — Profils normalisés internationaux AMH1n — Systèmes de messagerie — Messagerie commune —

Partie 1: Support de service MHS

Reference number
ISO/IEC ISP 10611-1:1994(E)

Contents

Foreword

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

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. In addition to developing International Standards, ISO/IEC JTC 1 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:

— OSI 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)*

Annexes A and B form an integral part of this part of ISO/IEC ISP 10611. Annexes C, D and E are for information only.

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.

An overview of the scope and applicability of the AMH1n set of profiles and of the structure of this multipart ISP is provided in annex E.

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 the Telecommunications Standardization Bureau of the ITU maintains a list of currently valid ITU-T 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 ITU-T Recommendations (as noted below) unless otherwise stated.

ISO 7498-2: 1989, *Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture.*

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(1992)]*

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(1992)]*

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(1992)]*

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(1992)]*

CCITT Recommendation X.400(1992), *Message handling system and service overview.*

CCITT Recommendation X.402(1992), *Message handling systems: Overall architecture.*

CCITT Recommendation X.411(1992), *Message handling systems: Message transfer system: Abstract service definition and procedures.*

CCITT Recommendation X.413(1992), *Message handling systems: Message store: Abstract service definition.*

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

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.

3.3 Profile object identifiers

Profiles that are specified in ISO/IEC ISP 10611 are identified by the object identifiers in table 1.

NOTE - These object identifiers are included for formal purposes and any use of them is not defined. They are not related to any implementation of messaging and do not appear in the protocols specified in this ISP.

Table 1 - Profile object identifiers

Profile	Object Identifier
AMH111	{ iso(1) standard(0) common-messaging(10611) message-transfer(3) normal-mode(1) }
AMH112	{ iso(1) standard(0) common-messaging(10611) message-transfer(3) x410-mode(2) }
AMH12	{ iso(1) standard(0) common-messaging(10611) mts-access(4) }
AMH13	{ iso(1) standard(0) common-messaging(10611) ms-access(5) }

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 Content
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 functional object 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 functional object - 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.

6.1 Content and encoded information types

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

6.2 Message length

If the implementation imposes any constraints on the size of the message content or envelope, then all such constraints shall be stated in the PICS.

NOTE - Implementors are advised to avoid constraining the size of messages as far as possible. For example, any constraint which prevents the transfer of a 2 Megaoctet message could cause problems when interworking with 1984 systems. Requirements will vary according to application and environment and could be much higher than 2 Megaoctets.

6.3 Number of recipients

It shall be stated in the PICS if there is any limit on the number of recipients that can be specified in a message envelope.

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 functional object. The following subclauses 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 functional object (i.e. MTA, MS or UA - whether as MTS-user or as MS-user is not distinguished), is given in table 2.

Table 2 - 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 Content (RoC)	Y	Y	Y
Security (SEC)	Y	Y	Y

Functional Group	MTA	MS	UA
Use of Directory (DIR)	Y	N	Y
84 Interworking (84IW)	Y	N	N[1]
NOTES 1 UA functionality may be further defined in content type-dependent profiles.			

The conformance requirements for support of the various functional groups, covering support of additional protocol elements and/or procedures, are specified in parts 3, 4 and 5 of this ISP, according to the protocol(s) to which each functional group relates.

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 1 - 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 subclauses 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 2 - 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.

A conforming implementation shall obey the rules specified in subclause 14.3.10 of ISO/IEC 10021-4.

Conformance to ISO/IEC ISP 10611 does not require any DL management capability other than as specified in subclause 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 subclause 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 Content (RoC)

The Return of Content FG covers support of the Return of Content 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, an MS or a UA. If an MTA supports the RoC FG and also supports message submission, then it shall also support the Return of Content EoS on submission.

NOTE - Return of content 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.

Table 3 summarizes the requirements of the security classes on an MTS-user and on an MTA.

Table 3 - 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.

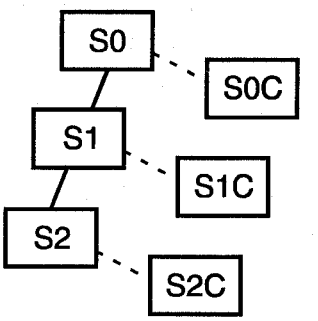

Figure 1 - Incremental functionality of the SEC security classes

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 4. 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 4 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 4 - 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 security class S0C security-class-S1 security-class-S1C security-class-S2 security-class-S2C	 { id-policy-identifier 0 0 } { id-policy-identifier 0 1 } { id-policy-identifier 1 0 } { id-policy-identifier 1 1 } { id-policy-identifier 2 0 } { id-policy-identifier 2 1 }
id-category-identifier	{ id-mhs-security 2 }
security-categories: private confidence commercial-in-confidence management-in-confidence personal-in-confidence	 { id-category-identifier 0 } { id-category-identifier 1 } { id-category-identifier 2 } { id-category-identifier 3 } { 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 functional objects are involved in the provision and use of each security service.

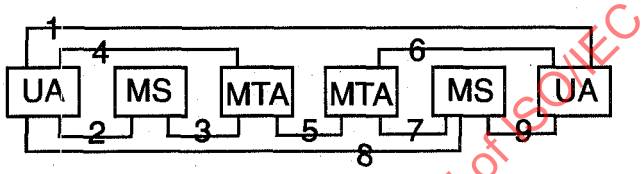

Figure 2 - Key to security class tables

7.7.3.1 Security class S0

Table 5 - 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	–	–	–	–	–	–	–	–

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
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 6 - 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

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
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 7 - 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 8 - 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 1 - 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 subclause 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. The use of a directory service to support distribution list processing is outside the scope of this version of ISO/IEC ISP 10611.

NOTE 2 - The MTS may also use a directory service to obtain information, for example, that may be used in the routeing 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 ITU 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 subclause 18.2 of ISO/IEC 10021-2.

NOTE - It is recommended that the alpha-2 form of the country-name attribute be used. It is recommended that the Printable String form of the administration-domain-name and private-domain-name attributes be used.

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 subclause 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 routeing and delivery.

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

8.3 Routeing 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 that supports 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 routeing 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.

For any MTA that supports message transfer, it shall be stated in the PICS whether rerouteing is supported.

For any MTA that supports message delivery, it shall be stated in the PICS which O/R address attributes may be used for registration of local MTS-users (and thus may be used for delivery determination) and any constraints (e.g. any limitations on the range of values, character repertoires, etc) which may apply.

8.4 Validation of O/R addresses

As specified in subclause 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 and that the originator-name is in fact an OR-address of the MTS-user submitting the message.

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.

Handling of other protocol violations will be a matter for local policy. Implementations are not required to perform protocol validation other than where it is required to take action based on such protocol elements.

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]					

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
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]	–	–	RED			m		
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 capability to generate the "prohibited" value is required for conformance to this ISP.

9 Support of this EoS is mandatory when the P3 protocol is supported for MTS access. In this case, the mechanism used is the P3 delivery-control operation. 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	m[3]	m[3]	m[2]	m[2]	m[2]	m[2]
Message Origin Authentication	m[4]	m[3]	m[2,4]	m[2]	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.

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 *MHS Implementors' Guide*, Version 11 (ITU Special Rapporteur's Group on Message Handling Systems and ISO/IEC JTC1/SC18/WG4 SWG on Messaging).

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 10021-1/Cor.6:1994

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 10021-2/Cor.5:1993

ISO/IEC 10021-2/Cor.6:1994

ISO/IEC 10021-2/Cor.7:1994

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 10021-4/Cor.6:1993

ISO/IEC 10021-4/Cor.7:1994

ISO/IEC 10021-4/Cor.8:1994

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

ISO/IEC 10021-5/Cor.6:1993

ISO/IEC 10021-5/Cor.7:1994

ISO/IEC 10021-1/Amd.2:1994

ISO/IEC 10021-2/Amd.1:1993

ISO/IEC 10021-2/Amd.2:1994

ISO/IEC 10021-4/Amd.1:1994

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
- misrouteing
- 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.

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.

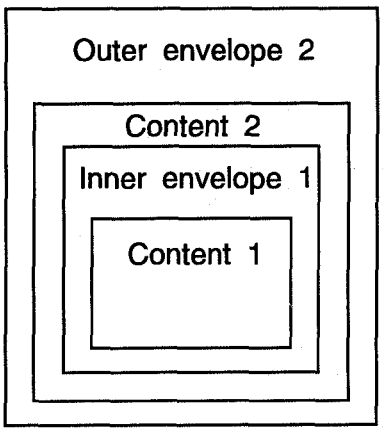

Figure C.1 - Double enveloping

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 routeing 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 routeing 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;