INTERNATIONAL STANDARDIZED PROFILE

ISO/IEC ISP 10611-1

Second edition
1997-12-15

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 10611-1:1997(E)

Documents
Document Sharing Hub

Full document details: ISO_IEC ISP 10611-1_1997

Contents

Page

Foreword iii

Introduction iv

1 Scope 1

2 Normative references 2

3 Definitions 2

4 Abbreviations 4

5 Conformance 5

6 Basic requirements 5

7 Functional groups 6

8 Naming and addressing 19

9 Error and exception handling 20

Annexes

A Elements of Service 21

B Amendments and corrigenda 30

C Secure messaging - rationale and implementation considerations 31

D Additional recommended practices for 1984 interworking 39

E AMH1 - overall scope and applicability 41

F Bibliography 45

© ISO/IEC 1997
All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from the publisher.

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

Printed in Switzerland

Documents
Document Sharing Hub

Full document details: ISO_IEC ISP 10611-1_1997

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 a 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);

— Open Systems Environment Implementors' Workshop (OIW).

This second edition cancels and replaces the first edition (ISO/IEC ISP 10611-1:1994), which has been technically revised. It also incorporates Technical Corrigendum 1:1996.

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 and AMH14 - MTS Access (P3) and MTS 94 Access (P3)*

— *Part 5: AMH13 - MS Access (P7)*

— *Part 6: AMH15 - MS 94 Access (P7)*

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

AVA Documents Document Sharing Hub

Full document details: ISO_IEC ISP 10611-1_1997

© ISO/IEC

Introduction

This part of 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. 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.

Documents
Document Sharing Hub

Full document details: ISO_IEC ISP 10611-1_1997

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 AMH14), ISO/IEC ISP 10611-5 (AMH13) and ISO/IEC ISP 10611-6 (AMH15), 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 ISO/IEC ISP 10611 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”.

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

Documents
Document Sharing Hub
Full document details: ISO_IEC ISP 10611-1_1997

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.

NOTES

1 - 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.

2 - Informative references are found in annex F.

ISO/IEC TR 10000-1:—[1], *Information technology - Framework and taxonomy of International Standardized Profiles - Part 1: General principles and documentation framework.*

ISO/IEC TR 10000-2:—[1], *Information technology - Framework and taxonomy of International Standardized Profiles - Part 2: Principles and Taxonomy for OSI profiles.*

ITU-T Recommendation F.400/X.400 (1996), *Message Handling Systems - System and service overview.*

ISO/IEC 10021-1:—[2], *Information technology - Message Handling Systems (MHS): System and service overview [see also ITU-T Recommendation F.400/X.400].*

ITU-T Recommendation X.402 (1995) | ISO/IEC 10021-2: 1996, *Information technology - Message Handling Systems (MHS): Overall architecture.*

ITU-T Recommendation X.411 (1995) | ISO/IEC 10021-4: 1997, *Information technology - Message Handling Systems (MHS): Message transfer system: Abstract service definition and procedures.*

ITU-T Recommendation X.413 (1995) | ISO/IEC 10021-5: 1996, *Information technology - Message Handling Systems (MHS): Message store: Abstract service definition.*

ITU-T Recommendation X.509 (1993) | ISO/IEC 9594-8: 1995, *Information technology - Open Systems Interconnection - 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.

---

[1] To be published. (Revision of ISO/IEC 10000:1995)
[2] To be published. (Revision of ISO/IEC 10021-1:1994)

Documents
Document Sharing Hub
Full document details: ISO_IEC ISP 10611-1_1997

3.1 General

3.1.1 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.

3.1.2 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.

3.2.1 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.

3.2.2 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.

3.2.3 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).

3.2.4 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.

3.2.5 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.

Documents
Document Sharing Hub
Full document details: ISO_IEC ISP 10611-1_1997

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) }
AMH14	{ iso(1) standard(0) common-messaging(10611) mts-95-access(6) }
AMH15	{ iso(1) standard(0) common-messaging(10611) ms-94-access(7) }

4 Abbreviations

84IW 84 Interworking
AA Auto-Annotation
AC Auto-Correlation
AD Auto-Deletion
AG Auto-Grouping
ALERT Alert
AMH Application Message Handling
ASN.1 Abstract Syntax Notation One
COMPUSEC Computer security
COMSEC Communications security
CV Conversion
DC Delivery Constraints
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
LOG Logging
MHS Message Handling Systems
MLS Multi-Level Security
MS Message store
MT Message transfer
MTA Message transfer agent
MTS Message Transfer System
ORAM ORAddress Matching
ORNM ORName Matching
OSI Open Systems Interconnection
PD Physical Delivery
PDAU Physical delivery access unit
RED Redirection
RED2 Redirection Instructions
RD Restricted Delivery
RoC Return of Content
SDM Storage of Draft Messages
SEC Security
SG Storage and Grouping
SPP Simple Protected Password
TRASH Trash
UA User agent

AVA Documents Document Sharing Hub

Full document details: ISO_IEC ISP 10611-1_1997

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.

Documents
Document Sharing Hub
Full document details: ISO_IEC ISP 10611-1_1997

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 and 3. Table 3 lists the functional groups which are only applicable when claiming conformance to AMH15.

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
Use of Directory (DIR)	Y	N	Y
84 Interworking (84IW)	Y	N	N[1]
Simple Protected Password (SPP)	Y	Y	Y
Redirection Instructions (RED2)	Y	N	Y
Delivery Constraints (DC)	Y	N	Y
Restricted Delivery (RD)	Y	N	Y

NOTES

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

AVA Documents Document Sharing Hub

Full document details: ISO_IEC ISP 10611-1_1997

Table 3 - Summary of AMH15 optional functional groups

Functional Group	MTA	MS	UA
ORAddress Matching (ORAM)	N	Y	Y
ORName Matching (ORNM)	N	Y	Y
Storage of Draft Messages (SDM)	N	Y	Y
Storage and Grouping (SG)	N	Y	Y
Alert (ALERT)	N	Y	Y
Auto-Annotation (AA)	N	Y	Y
Auto-Grouping (AG)	N	Y	Y
Trash (TRASH)	N	Y	Y
Auto-Deletion (AD)	N	Y	Y
Auto-Correlation (AC)	N	Y	Y
Logging (LOG)	N	Y	Y

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, 5 and 6 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.

Documents
Document Sharing Hub
Full document details: ISO_IEC ISP 10611-1_1997

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 OR-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.

Documents
Document Sharing Hub

Full document details: ISO_IEC ISP 10611-1_1997

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.

NOTE - A separate Functional Group is defined for Simple Protected Password, since it was introduced in the base standard in the 1995-1996 publication.

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

Documents
Document Sharing Hub
Full document details: ISO_IEC ISP 10611-1_1997

Table 4 - Overview of the SEC security classes

Security Class	MTS-user	MTA
Basic		Supports relay of security EoS
S0	Content integrity Origin authentication (end-to-end)	Supports submission and delivery of security EoS
S1	As S0 plus: Proof of delivery 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.

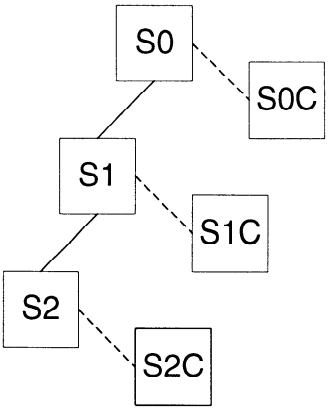

Figure 1 - Incremental functionality of the SEC security classes

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 5. 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 5 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.

Documents
Document Sharing Hub
Full document details: ISO_IEC ISP 10611-1_1997

Table 5 - 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-no-PoD security-class-S0C-no-PoD security-class-S1 security-class-S1C security-class-S2 security-class-S2C	 { id-policy-identifier 0 0 0 } { id-policy-identifier 0 1 0 } { 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.

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.

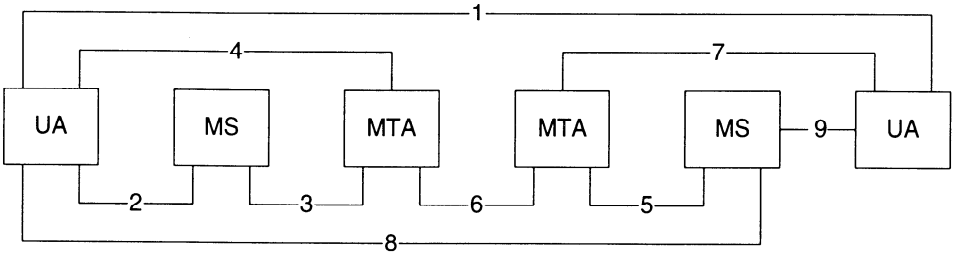

Figure 2 - Key to security class tables

Documents
Document Sharing Hub
Full document details: ISO_IEC ISP 10611-1_1997

7.7.3.1 Security class S0

Table 6 - 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	o	–	–	–	–	–	–	o	–
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	–
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	–	–	–	–	–	–	–

AVA Documents Document Sharing Hub

Full document details: ISO_IEC ISP 10611-1_1997