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

Output from the June 1994 Open Systems Environment Implementors' Workshop (OIW)

SIG Chair: **Chris Bonatti, Booz • Allen & Hamilton**
SIG Editor: **Chris Bonatti, Booz • Allen & Hamilton**

Foreword

The text in this chapter specifies the North American requirements for use of the MHS ISPs. It also specifies any additional requirements and Recommended Practices that are beyond the scope of the ISPs.

Table of Contents

List of Figures

List of Tables

Part 8 Message Handling Systems

0 Introduction

1 Scope

2 References

2.1 CCITT

2.2 ISO

Editor's Note: **[**The following reference is in addition to the contents of the same chapter and clause of the OIW Stable Implementation Agreements. It is anticipated that the referenced chapter will be created at the March 1994 OIW Plenary.**]**

Application Layer - MHS

OIW SIA Chapter ZZ - Working Draft ISP 12063 *Information Processing Systems - International Standardized Profiles AMH3n - Message Handling Systems - EDI Messaging*.

2.3 IETF Documents

Requests for Comment (RFCs)

RFC 822 *Standard for the format of ARPA Internet text messages*, August 1982.

RFC 1327 *Mapping between X.400(1988) / ISO 10021 and RFC 822*, May 1992.

RFC 1344 *Implications of MIME for Internet Mail Gateways*, June 1992.

RFC 1421 *Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures*, February 1993.

RFC 1422 *Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management*, February 1993.

RFC 1423 *Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers*, February 1993.

RFC 1425 *SMTP Service Extensions*, February 1993.

RFC 1427 *SMTP Service Extension for Message Size Declaration*, February 1993.

RFC 1428 *Transition of Internet Mail from Just-Send-8 to 8bit-SMTP/MIME*, February 1993.

RFC 1437 *The Extension of MIME Content-Types to a New Medium*, April 1993.

RFC 1465 *Routing Coordination for X.400 MHS Service Within a Multi Protocol / Multi Network Environment Table Format V3 for Static Routing*, May 1993.

RFC 1494 *Equivalences between 1988 X.400 and RFC-822 Bodies*, August 1993.

RFC 1495 *Mapping between X.400 and RFC-822 Message Bodies*, August 1993.

RFC 1521 *MIME (Multipurpose Internet Mail Extensions) Part One: Mechanisms for Specifying and Describing the Format of Internet Message Bodies*, September 1993.

RFC 1522 *MIME (Multipurpose Internet Mail Extensions) Part Two: Message Header Extensions for Non-ASCII Text*, September 1993.

RFC 1563 *The text/enriched MIME Content-type*, January 1994.

Editor's Note - Consider adopting the following references in the future.

RFC 821 *Simple Mail Transfer Protocol*, August 1982.

RFC 1424 *Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services*, February 1993.

RFC 1426 *SMTP Service Extension for 8bit-MIMEtransport*, February 1993.

RFC 1590 *Media Type Registration Procedure*, March 1994.

3 Status

4 Taxonomy and Functional Groups

4.1 AMH1

4.2 AMH2

4.3 AMH3

The AMH3n set of profiles is applicable to end systems operating in an Open Systems Interconnection (OSI) environment which form part of a distributed Message Handling Systems (MHS) environment and which provide an EDI messaging service.

The AMH31 profile specifies the EDI Messaging content (Pedi "protocol") which is carried end-to-end (i.e., UA-to-UA) by the MHS protocols (i.e., P1, P3, and P7).

The remaining AMH3n profiles cover the other aspects of an EDI MHS environment, specifying additional requirements to those specified in the AMH1n Common Messaging set of profiles as appropriate to support an EDIMG service:

- AMH32 - EDI Requirements for Message Transfer (P1) - any additional MTA capabilities related to message transfer which are specific to support of an EDIMG environment (i.e., additional to the requirements of AMH11)

- AMH33 - EDI Requirements for MTS Access (P3) - any additional MTA and MTS-user capabilities related to MTS access which are specific to support of an EDIMG environment (i.e., additional to the requirements of AMH12)

- AMH34 - EDI Requirements for MS Access (P7) - any additional MS and MS-user capabilities related to MS access which are specific to support of an EDIMG environment (i.e., additional to the requirements of AMH13)

Each AMH3n profile specifies the conformance requirements for all relevant MHS functional objects (i.e., MTA, UA, MS). Two or more AMH3n profiles can be combined to establish the conformance requirements for the various physical configurations that may be achieved within the scope of the MHS base standards, as illustrated in the following diagram.

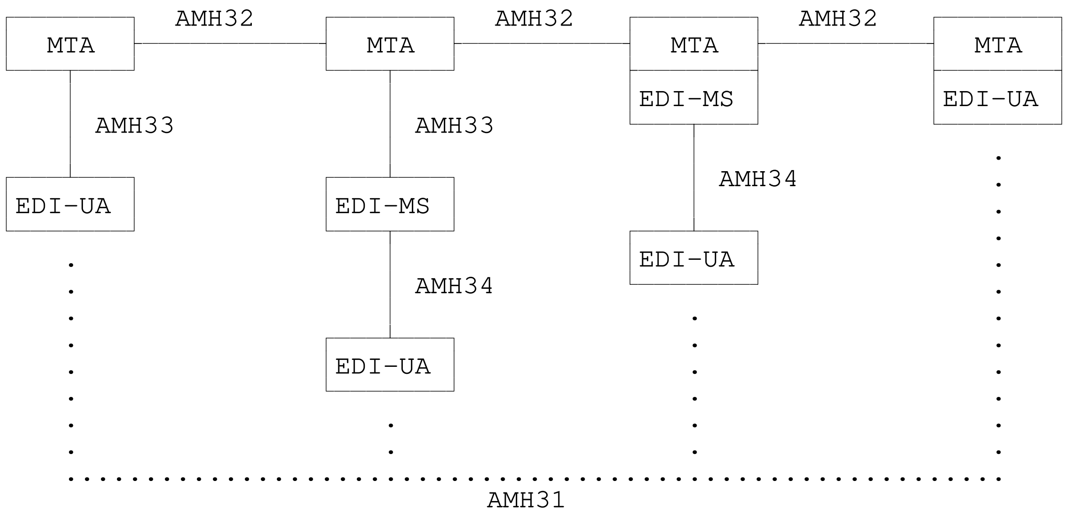

Figure 3 - Combinations of AMH3n Profiles

The AMH3n set of profiles is specified as a multipart ISP consisting of the following parts:

Part 1: EDI MHS service support.

> A common text part which provides functional description and specification of EDIMG specific MHS service support and associated functionality as covered by the AMH3n set of profiles. It identifies what additional service support and functionality can be supported by each type of MHS component in an EDIMG environment (i.e. also covering the services supported by an EDI UA, plus any additional MTA and MS aspects such as EDI body part conversion), divided into basic requirements and zero or more optional functional groups (see AMH1n). The specification in this part is designed for reference by the following parts (which specify conformance requirements by protocol for each MHS component) and is additional to the protocol-specific requirements specified in those parts. Thus, although this part contains normative requirements, there is no separate conformance to this part (i.e. it is not identified in the MHS taxonomy) since such requirements are only significant when referenced in the context of a particular protocol profile.

Part 2: EDI Content.

> This part covers EDI UA functionality. It specifies support of the EDI content 'protocol' in terms of basic requirements and optional functional groups and defines conformance requirements for an EDI UA with respect to support of EDI content and associated functionality (by reference to the common EDIMG specifications in part 1).

Part 3: AMH32 - EDI requirements for Message Transfer (P1).

> This part covers message transfer between MTAs using the P1 Message Transfer Protocol to support an EDIMG environment. It specifies any additional P1 support to that specified in AMH1n and defines conformance requirements for an MTA which supports EDIMG transfer with respect to support of P1 and associated functionality (requiring conformance to AMH11 and by reference to the common EDIMG specifications in part 1).

Part 4: AMH33 - EDI requirements for MTS Access (P3).

This part covers access to an MTS using the P3 MTS Access Protocol to support an EDIMG environment. It specifies any additional P3 support to that specified in AMH1n and defines conformance requirements for an MTA which supports remote access for EDI use, and for a remote MTS-user in an EDIMG context (i.e. EDI UA or MS), with respect to support of P3 and associated functionality (requiring conformance to AMH12 and by reference to the common EDIMG specifications in part 1).

Part 5: AMH34 - EDI requirements for Enhanced MS Access (P7).

This part covers access to an MS using the P7 MS Access Protocol to support an EDIMG environment. It specifies any additional P7 support to that specified in AMH1n and defines conformance requirements for an MS which supports remote access for EDI use, and for a remote MS-user in an EDIMG context (i.e. EDI UA), with respect to support of P7 and associated functionality (requiring conformance to AMH13 and by reference to the common EDIMG specifications in part 1).

5 Conformance

"MHS-88-MTA-Gateway" specifies a remote Message Store that serves a remote User Agent. If the MS is a CCITT 1988 Interpersonal Messaging (IPM) MS, it must conform to AMH24 and AMH22 as enhanced by section 8 of this Agreement. If the MS is an Electronic Data Interchange (EDI) MS, it must conform to AMH34 and AMH33 as enhanced by section 9 of this Agreement. If the MS supports any other content type, the implementation must conform to both AMH12 and AMH13 and specify the content type(s) supported, if any, in section A.1.3 of the PICS for AMH13.

"MHS-88-UA-Gateway-P3" specifies a remote User Agent that is co-located with a Message Store. For conformance purposes this is the same as the "MHS-88-Remote UA-P3."

"MHS-88-UA-Gateway-P7" specifies a remote User Agent that is co-located with a Message Store. For conformance purposes this is the same as the "MHS-88-Remote UA-P3."

Table 1 - MHS Configurations (concluded)

Entity	Protocol(s)	Conformance
MHS-88-MTA-Gateway	P1 + possible content types IPMS EDI other	AMH11 + Section 6 AMH21 + AMH22 + Section 8 AMH31 + AMH32 + Section 9 details in PICS in AMH11 (A.3.2) Section 10

MHS-88-UA- Gateway-P3	P3 + possible content types IPMS EDI other	AMH12 + Section 6 AMH21 + AMH23 + Section 8 AMH31 + AMH33 + Section 9 details in PICS in AMH12 (A.3.2) Section 10
MHS-88-UA- Gateway-P7	P7 + possible content types IPMS EDI other	AMH13 + Section 6 AMH21 + AMH24 + Section 8 AMH31 + AMH34 + Section 9 detail in PICS in AMH12 (A.3.2) and AMH13 (A.3) Section 10

6 Common Messaging

7 MHS Management

NOTE - For further study.

8 IPM Service

9 EDI Messaging Service

9.1 Introduction

This clause specifies EDI conformance requirements. Conformance to AMH3 is required, as well as support of the ANSI X12 functional group. Other regional requirements are specified in clauses 9.2 and 9.3.

Criticality mechanisms must be supported for all extension fields.

9.2 P(EDI) Protocol

This clause defines the additional requirements for EDI-UA support of the EDI protocol (Pedi). The following tables define differences from the requirements of the AMH3 ISP, Part 2, Annex A.

Table 13 - Delta to pDISP 12063-2, Annex A, Clause A.2.4.1: EDIN Common Fields

Ref	Element	Origination		Reception		Notes
		Base	Profile	Base	Profile	
3	first-recipient		m			

Table 14 - Delta to pDISP 12063-2, Annex A, Clause A.2.4.3: NN Fields

Ref	Element	Origination		Reception	
		Base	Profile	Base	Profile
2.3	nn-pdau-reason-code		o		
2.3.1	nn-pdau-basic-code		m		
2.3.2	nn-pdau-diagnostic		m		

Table 15 - Delta to pDISP 12063-2, Annex A, Clause A.2.4.4: FN Fields

Ref	Element	Origination		Reception	
		Base	Profile	Base	Profile
3.1.3	fn-security-check			o	o
3.3	fn-pdau-reason-code		o		
3.3.1	fn-pdau-basic-code		m		
3.3.2	fn-pdau-diagnostic		m		

9.3 EDI MS Attributes

This clause defines the additional requirements for EDI-UA and EDI-MS support of the EDI protocol attributes. The following tables define differences from the requirements of the AMH3 ISP, Part 5, Annexes A and B.

Table 18 - Delta to pDISP 12063-5, Annex A: EDI Forwarding class AT and class MF

Ref	Attribute	UA Base	MS Base
	date-and-time-of-preparation		m

Table 19 - Delta to pDISP 12063-5, Annex B, Clause B.1.12: EDI-Specific Attributes

Ref	Attribute	Profile	
		EDI-UA	EDI-MS
	application-reference		o
	edi-notification-requests-for-this-recipient		o
	edim-body-part	o	o
	expiry-time		o
	fn-reason-code		o
	fn-supplementary-information		o
	forwarded-to		o
	interchange-length		o
	nn-reason-code		o
	nn-supplementary-information		o
	notification-time		o
	originator		o
	pn-supplementary-information		o
	processing-priority-code-for-this-recipient	m	
	related-messages		o
	service-string-advice		o
	test-indicator-for-this-recipient	m	
	this-recipient		o

Table 20 - Delta to pDISP 12063-5, Annex B, Clause B.2.1 EDI Forwarding class AT and class MF

Ref	Attribute	Profile	
		EDI-UA	EDI-MS
	edim-body-part	m	m
	incomplete-copy	m	m
	responsibility-forwarded	m	
	responsibility-passing-allowed-for-this-recipient	m	

Table 21 - Delta to pDISP 12063-5, Annex B, Clause B.2.2.1 EDI Security (Class A and B)

Ref	Attribute	Profile	
		EDI-UA	EDI-MS
	edi-notification-security-for-this-recipient	m	
	edi-reception-security-for-this-recipient	m	

Table 22 - Delta to pDISP 12063-5, Annex B, Clause B.2.2.2 EDI Security (Class C)

Ref	Attribute	Profile	
		EDI-UA	EDI-MS
	edi-application-security-elements	m	
	edi-application-security-extensions	m	

Table 23 - Delta to pDISP 12063, Part 5, Annex B, Clause B.2.3 EDI Multi-Part Body (MPB)

Ref	Attribute	Profile	
		EDI-UA	EDI-MS
	cross-referencing-information	o	o
	edim-synopsis		o

10 Gateways

Gateways are functional objects which provide interworking between two instances of systems from similar classes of systems. For example, the functional object that provides interworking between X.400-based messaging system and an Internet-based messaging system is a gateway. It is the intent of these agreements to identify common practices for gateways where one system is always an X.400-based messaging system and the other system is a publicly available standards-based messaging system.

The definition of gateways should consider the following:

- the semantic mapping between types of information objects in each system, e.g., what does the semantics of the message and delivery report map into;

- the semantic mapping of the elements of service between the two systems, e.g., what does the semantics of the priority map into;

- are addressing forms of each system supported in the other system or is a directory-based address mapping function required; and,

- are operational aspects of each system mapable, e.g., service billing, settlements, message tracing, auditing, etc.

10.1 X.400 - Internet Messaging Gateway

A gateway providing interworking between X.400-based messaging system and an Internet-based messaging system should consider the following:

- the basic definition of Internet messaging (mail) is defined by RFC 822, the privacy enhancements (PEM) are defined in RFC , service extensions are defined in RFC 1425, RFC 1427 and RFC 1428, the multipurpose extensions (MIME) are defined in RFC 1521, RFC 1522, RFC 1563 and RFC 1437 and the implications for gateways is described in RFC 1344, the handling of non-ASCII information is defined in RFC 1522, routing coordination is described in RFC 1465, equivalences and mapping between message bodies is described in RFC 1494 and RFC 1495; and,

- the mapping between X.400 (1988) and RFC 822 is defined in RFC 1495 and RFC 1327.

Annex A (normative)

Naming, Addressing and Routing

Annex B (normative)

IPM Body Part Support

Annex C (normative)

Object Identifiers

Annex D (informative)

Interpretation of Elements of Service

Annex E (informative)

Recommended Practices

E.7 Selection of OR Name Attributes

E.7.2 Use of Domain Defined Attributes

To promote interoperability between 1984 and 1988 systems, when any 1988 O/R name contains Terminal Type attribute it can be downgraded to a DDA. The DDA type of "T-TY" should be used for the Terminal Type attribute. Wherever possible this DDA should be added by the originating UA to avoid conversion problems.

E.10 Reliable Transfer Service and Protocol

E.10.1 X.410-1984 Mode

E.10.1.1 Use of Session Services

The 1988 definition of the Reliable Transfer protocol (Recommendation X.228, 1988) is not bit-compatible with the 1984 version (X.410), however it was the intent for them to be bit-compatible. To make the 1988 version compatible with the 1984 version, it is recommended that implementations supporting the RTS 1984-mode apply the 1984 definition of the **CallingSSUserReference** for generating a value for the Calling SS User Reference field of the Session Connection Identifier parameter of the S-CONNECT service. This definition is:

```
CallingSSuserReference  ::=  CHOICE  {
                               -- local matter, solely in X.410-1984 mode
                               OCTET STRING -- required in normal mode -- }
```

E.10.1.2 RTTR Encoding

The encoding of the RTTR APDU in X.410 mode should omit the tag and length octets in accordance with CCITT X.410-1984.

E.10.2 Normal Mode

In normal mode, the total number of octets of the RTTRapdu (including any tag and length octets) is constrained by the RTSE checkpoint value.

Annex F (informative)

Bibliography

Annex G (informative)

Defense Message Handling Profiles

Annex H (informative)

Management Domains