



ICAO

Doc 9880

Technical Specifications for ATN using ISO/OSI Standards and Protocols

Second edition, 2016

Part II – Ground-Ground Applications —
Air Traffic Services Message Handling Services (ATSMHS)

Approved by and published under the authority of the Secretary General

INTERNATIONAL CIVIL AVIATION ORGANIZATION **Documents**



Document Sharing Hub

Copyright International Civil Aviation Organization

Provided by IHS Markit under license with ICAO
No reproduction or networking permitted without license from IHS

Full document details: ICAO 9880 PART II 2016

Licensee=/, User=
Not for Resale,

Doc 9880
AN/466



Manual on Detailed Technical Specifications for the Aeronautical Telecommunication Network (ATN) using ISO/OSI Standards and Protocols

**Part II — Ground-Ground Applications —
Air Traffic Services Message Handling
Services (ATSMHS)**

Second Edition — 2016

International Civil Aviation Organization

AVA **Documents**
Document Sharing Hub

Published in English only by the
INTERNATIONAL CIVIL AVIATION ORGANIZATION
999 Robert-Bourassa Boulevard, Montréal, Quebec, Canada H3C 5H7

For ordering information and for a complete listing of sales agents
and booksellers, please go to the ICAO website at www.icao.int

**Doc 9880, *Manual on Detailed Technical Specifications
for the Aeronautical Telecommunication Network (ATN)
using ISO/OSI Standards and Protocols*
Part II, *Ground-Ground Applications —
Air Traffic Services Message Handling Services (ATSMHS)***
Order Number: 9880PII
ISBN 978-92-9258-141-1

© ICAO 2017

All rights reserved. No part of this publication may be reproduced, stored in a
retrieval system or transmitted in any form or by any means, without prior
permission in writing from the International Civil Aviation Organization.

AMENDMENTS

Amendments are announced in the supplements to the *Catalogue of ICAO Publications*; the Catalogue and its supplements are available on the ICAO website at www.icao.int. The space below is provided to keep a record of such amendments.

RECORD OF AMENDMENTS AND CORRIGENDA

[illegible][illegible]

TABLE OF CONTENTS

	<i>Page</i>
Foreword	(vii)
Acronyms	(ix)
Chapter 1. Introduction	1-1
1.1 Overview	1-1
1.2 End systems providing the ATSMHS	1-2
1.3 Terminology	1-2
Chapter 2. System Level Provisions	2-1
2.1 ATSMHS users	2-1
2.2 AMHS model	2-1
2.3 Organization of the AMHS	2-3
2.4 AMHS management domain configurations	2-4
2.5 Naming and addressing principles	2-4
2.6 AMHS routing and re-routing	2-9
2.7 AMHS traffic logging upon origination	2-9
Chapter 3. ATSMHS Specification	3-1
3.1 ATS message user agent specification	3-1
3.2 ATS message server specification	3-8
3.3 Parameters	3-12
3.4 Subsetting rules	3-16
Chapter 4. AFTN/AMHS Gateway Specification	4-1
4.1 General	4-1
4.2 AFTN/AMHS gateway components	4-1
4.3 General functions	4-7
4.4 AFTN to AMHS conversion	4-11
4.5 AMHS to AFTN conversion	4-34

FOREWORD¹

This manual contains the detailed technical specifications for the ATN based on relevant standards and protocols established for open systems interconnection (OSI) by the International Organization for Standardization (ISO) and the Telecommunication Standardization Sector of the International Telecommunication Union (ITU-T). A separate manual, the *Manual on the Aeronautical Telecommunication Network (ATN) using Internet Protocol Suite (IPS) Standards and Protocols* (Doc 9896), addresses detailed technical specifications for the ATN based on standards developed for the IPS by the Internet Society (ISOC). Standards and Recommended Practices (SARPs) for the ATN/IPS are contained in Annex 10 — *Aeronautical Telecommunications*, Volume III — *Communication Systems*.

Editorial practices in this manual are as follows:

- The detailed technical specifications in this manual that include the operative verb “shall” are essential to be implemented to secure proper operation of the ATN.
- The detailed technical specifications in this manual that include the operative verb “should” are recommended for implementation in the ATN. However, particular implementations may not require this specification to be implemented.
- The detailed technical specifications in this manual that include the operative verb “may” are optional.

This manual is published in the following parts:

- Part I: Air-Ground Applications (replaces Doc 9705, Sub-volume II)
- Part II: Ground-Ground Applications — Air Traffic Services Message Handling Services (ATSMHS) (replaces Doc 9705, Sub-volume III)
- Part III: Upper Layer Communications Service (ULCS) and Internet Communications Service (ICS) (replaces Doc 9705, Sub-volume IV and Sub-volume V)
- Part IV: Directory Services, Security Services and Systems Management (replaces Doc 9705, Sub-volumes I, VI, VII, VIII and IX)

The ATSMHS shall be implemented in conformity with Part II, which is structured as follows:

- Chapter 1 INTRODUCTION contains the overview, a summary of the functionalities offered by the ATSMHS and the terminology applied
- Chapter 2 SYSTEM LEVEL PROVISIONS, provides a high-level specification of the application and the environment in which it operates
- Chapter 3 ATS MESSAGE HANDLING SERVICE SPECIFICATION, provides the detailed specification of the service and protocol requirements for each type of ATN End System (ATS message)

¹ The first edition of this manual amended and replaced the third edition of the *Manual of Technical Provisions for the Aeronautical Telecommunication Network (ATN)* (Doc 9705).

user agent and ATS message server) implementing the ATSMHS

Chapter 4 AFTN/AMHS GATEWAY SPECIFICATION, provides the detailed specification of an AFTN/AMHS gateway and of the related functional requirements such as conversion

ACRONYMS

The acronyms used in this manual are defined as follows:

ACSE	Association control service element
ADMD	Administration management domain
AF	AFTN-form (address)
AFTN	Aeronautical fixed telecommunication network
AMHS	ATS message handling system
ASN.1	Abstract syntax notation One
ASP	Signature generation primitive
ATN	Aeronautical telecommunication network
ATS	Air traffic services
ATSMHS	ATS message handling services
AU	Access unit
AVP	Signature verification primitive
BC	Business class (functional group)
BER	Basic encoding rules
CAAS	Common AMHS addressing scheme
CCITT	Consultative Committee of International Telegraph and Telephone
CIDIN	Common ICAO data interchange network
COTP	Connection-oriented transport protocol
CR	Carriage return
CRL	Certificate revocation list
DAP	Directory access protocol
DER	Distinguished encoding rule
DIR	Use of directory (functional group)
DL	Distribution list
DUA	Directory user agent
ECDSA	Elliptic curves digital signature algorithm
FG	Functional group
FT	Filing time
FTBP	File transfer body part
IA-5	International Alphabet No. 5
IA5IRV	International Alphabet No. 5 International Reference Version
ICS	Internet communications service
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IHE	IPM heading extension
IPM	Interpersonal message
IPN	Interpersonal notification
IPS	Internet protocol suite
ISO	International Organization for Standardization
ISP	International standardized profile
ISPICS	ISP implementation conformance statement
IPv4	Internet protocol version 4
IPv6	Internet protocol version 6
ITA-2	International Telegraph Alphabet No. 2

ITU	International Telecommunication Union
ITU-T	International Telecommunication Union — Telecommunications Standards
LF	Line feed
MD	Management domain
MF	MHS-form (address)
MHS	Message handling system
MOTIS	Message-oriented text interchange system
MS	Message store
MT	Message transfer
MTA	Message transfer agent
MT-EoS	Message transfer elements of service
MTS	Message transfer service
OHI	Optional heading info
OID	Object identifier
OR, O/R	Originator/recipient
PDAl	Predetermined distribution addressee indicator
PRL	Profile requirement list
PRMD	Private management domain
RFC	Request for change (issued by the IETF)
RER	Residual error rate
RN	Receipt notification
RTSE	Reliable transfer service element
SEC	Security (functional group)
SHA	Secure hash algorithm
SOH	Start of header
STX	Start of text
SOC	System 0 condition
TCP	Transmission control protocol
TSAP	Transport service access point
UA	User agent
UTC	Coordinated universal time
XF	Translated-form (address)
XMIB	Cross-domain management information base



Chapter 1

INTRODUCTION

1.1 OVERVIEW

1.1.1 The ATSMHS application, formerly known as the ATS message service, allows ATS messages to be exchanged between service users.

1.1.2 The ATSMHS application aims to provide generic message services over the ATN internet. It may in turn be used as a communication system by user-applications communicating over the ATN. This may be achieved, for instance, by means of application programme interfaces with the ATSMHS.

1.1.3 The ATSMHS is provided by the implementation over the ATN internet communication services of the message handling systems specified in ISO/IEC 10021 and CCITT or ITU-T X.400, complemented by the additional requirements specified in this manual. The ISO/IEC MOTIS international standards and the CCITT X.400 series of recommendations (1988 or later) are in principle aligned with each other. However, there are a small number of differences between these international standards and ISPs where applicable. Where necessary, for example, for reasons of interworking or to point out differences, reference is also made to the relevant X.400 recommendations.

1.1.4 Two levels of service are defined within the ATSMHS:

- a) the basic ATSMHS; and
- b) the extended ATSMHS.

1.1.5 The basic ATSMHS is based on the first version of the ISO/IEC ISPs, published in 1994 and based on the ISO/IEC 10021:1990 set of standards. The extended ATSMHS is based on the third version of the ISO/IEC ISPs, published in 2003 and based on the ISO/IEC 10021:2003 set of standards.

1.1.6 Both levels of service are compatible with one another. The extended ATSMHS is functionally a superset of the basic ATSMHS and is backward compatible with the basic ATSMHS.

1.1.7 The basic ATSMHS meets the basic requirements of the message handling systems profiles published by ISO/IEC as ISPs and incorporates additional features to support the service offered by the AFTN. The extended ATSMHS includes supplementary functions to provide a secure message service to allow for the use of the ATN directory. The ATSMHS is further specified in Chapter 3, including which ISPs apply in this context.

1.1.8 It is intended that the extended ATSMHS will eventually be supported by all ATSMHS users, so that the basic ATSMHS will no longer be required. However, the latter may be maintained for transition purposes as long as required.

1.2 END SYSTEMS PROVIDING THE ATSMHS

1.2.1 The set of end systems providing the ATSMHS is collectively denominated as the AMHS.

1.2.2 Three types of ATN end systems are defined in this manual:

- a) the ATS message server;
- b) the ATS message user agent; and
- c) the AFTN/AMHS gateway.

1.2.3 Connections may be established over the ATN ICS or using the IPS between any pair constituted of these ATN end systems and listed in Table 1-1.

Table 1-1. Communications between ATN end systems implementing the ATSMHS

<i>ATN end system 1</i>	<i>ATN end system 2</i>
ATS message server	ATS message server
ATS message server	AFTN/AMHS gateway
ATS message server	ATS message user agent
AFTN/AMHS gateway	AFTN/AMHS gateway

1.2.4 The CIDIN/AMHS gateway defined in earlier ATN technical provisions can be implemented by means of an AFTN/AMHS gateway when the CIDIN is used in support of the AFTN application only. For this reason, the specification of the CIDIN/AMHS gateway has been removed from this manual.

1.3 TERMINOLOGY

1.3.1 The following terminology applies in this manual:

AFTN acknowledgement message. An AFTN service message acknowledging the receipt of an AFTN message, of which priority indicator has the value “SS”.

Direct AMHS user. An ATSMHS user who engages in the ATSMHS at an ATS message user agent. A direct AMHS user may belong to two subgroups as follows:

Human users who interact with the ATSMHS by means of an ATS message user agent connected to an ATS message server.

Host users which are computer applications running on ATN end systems and interacting with the ATSMHS by means of application programme interfaces.

Indirect AMHS user. An ATSMHS user at an AFTN station using an AFTN/AMHS gateway to communicate with other ATSMHS users.

Subject AFTN message. An AFTN message which causes an AFTN service message or an AMHS report to be generated.

Subject AMHS message. An AMHS message which causes an AFTN service message or an AMHS report to be generated.

Subject IPM. The IPM which is the content of an AMHS message and which causes an AMHS RN to be generated.

Unknown address AFTN service message. An AFTN service message requesting correction by the originator of a message received with an unknown addressee indicator.

1.3.2 The classifications defined in the ISPs apply for expressing conformance requirements (i.e. static capability) in this manual. The ISP classifications refine the ISO/IEC 9646-7 classification to include different levels of mandatory support, depending on the level of functionality to be supported by the considered message handling system. These classifications include the following elements, for which the complete definition may be found in each referenced ISP:

- a) **mandatory (full) support (M);**
- b) **mandatory minimal support (M-);**
- c) **mandatory O/R name minimal support (M1)** (see ISO/IEC ISP 12062-2);
- d) **optional support (O);**
- e) **conditional support (C);**
- f) **out of scope (I);** and
- g) **not applicable (-).**

1.3.3 The following classification applies for expressing dynamic behaviour requirements (i.e. the action performed by the ATN end system) related to parameters or elements in PRLs included in Chapter 4 for the specification of the AFTN/AMHS gateway:

- a) **generated (G):** used to describe the generation of an AMHS or AFTN information object. It means that the element is generated by the AFTN/AMHS gateway. The value of the element is based on parameters related to the AFTN/AMHS gateway itself or takes a pre-determined value and does not depend on the value of an element of the information object received by the AFTN/AMHS gateway which caused the current generation of an information object. If an element comprises several components, then the element is classified as generated if at least one of its components is generated, and the others are either generated or excluded. The generation of message handling system parameters applies to abstract-values and does not constrain the ASN.1 encoding. In particular, elements generated with ASN.1 DEFAULT abstract-values may, but need not, be encoded;
- b) **optionally generated (G1):** used with the same meaning as generated (G), with the exception that the generation of the element is optional, the decision being a matter of policy local to the management domain operating the AFTN/AMHS gateway;
- c) **conditionally generated (G2):** used only to describe the generation of an AMHS report or RN element. It means, for a report generation, that the element is generated in the report or RN based on some condition related to the subject AMHS message being true. If the element is generated, it takes

a value derived from elements present in the received AMHS information object which caused the generation of the report or RN;

- d) **translated** (T): used to describe either the generation of an AMHS or AFTN information object or the use of a received information object. It means that the element is translated by the AFTN/AMHS gateway, using a dependence relationship between the value of an element of the received information object and the value of the translated element in the generated information object. If an element comprises several components, then the element is classified as translated if at least one of its components is translated, and the others are either generated or excluded in generation, discarded or out of scope in reception;
- e) **conditionally translated** (T1): used with the same meaning as translated (T), with the exception that the translation of the element is subject to some condition being true, e.g. the presence of an optional element in the received information object;
- f) **discarded** (D): used to describe the use of a received AMHS or AFTN information object. It means that the value of the element is not used by the message transfer and control unit when generating the elements of the information object converted from the received information object, and that the semantic information conveyed in the element is discarded during the process of conversion in the AFTN/AMHS gateway. However, the presence or value of the element may be used by the message transfer and control unit for purposes other than conversion, such as report generation and logging;
- g) **excluded** (X): used to describe either the generation of an AMHS or AFTN information object or the use of a received information object. Upon generation of an information object, it means that the element is not used or present in the generated information object. Upon reception of an AMHS information object, it means that the presence of the element causes rejection of the information object and generation of an AMHS non-delivery report;
- h) **out of scope** (I) or **not-applicable** (-): used to describe the use of a received information object, when the element is either a format element which cannot be processed in any way or an element which is not in the scope of the section, but which presence is included in the ISPICS serving as a basis for the mapping specification.

Chapter 2

SYSTEM LEVEL PROVISIONS

2.1 ATSMHS USERS

- 2.1.1 Direct AMHS users shall use either the basic ATSMHS or the extended ATSMHS at an ATS message user agent.
- 2.1.2 Indirect AMHS users shall use only that part of the ATSMHS which corresponds to AFTN functionalities by using the interworking capability provided by an AFTN/AMHS gateway as specified in Chapter 4.

2.2 AMHS MODEL

2.2.1 AMHS functional model

2.2.1.1 Model components

2.2.1.1.1 The systems comprising the AMHS shall themselves be comprised of the following functional objects, the general role of which is described in ISO/IEC 10021-2 and ISO/IEC 9594-2:

- a) message transfer agent(s) (MTA);
- b) user agent(s) (UA);
- c) message store(s) (MS);
- d) access unit(s) (AU); and
- e) directory user agent(s) (DUA).

2.2.1.1.2 The ISO/IEC 10021 elements of service and protocols used by these functional objects are specified in Chapters 3 and 4.

2.2.1.1.3 The ISO/IEC 9594 services and protocols used by these functional objects are specified in Part IV.

2.2.1.1.4 The DUA is an intrinsic part of the extended ATSMHS. However, they also belong to the ATN directory as specified in Part IV.

2.2.1.2 ATS message server

2.2.1.2.1 An ATS message server shall include an MTA and optionally one or several MS, as specified in 3.2.2 to 3.2.4.

2.2.1.2.2 For the support of the extended ATSMHS, an ATS message server shall include a DUA as specified in §3.2.5.

2.2.1.3 ATS message user agent

2.2.1.3.1 An ATS message user agent shall include a UA as specified in §3.1.2 to §3.1.4.

2.2.1.3.2 For the support of the extended ATSMHS, an ATS message user agent shall include a DUA as specified in §3.1.5.

2.2.1.4 AFTN/AMHS gateway

2.2.1.4.1 An AFTN/AMHS gateway shall include an MTA, which is part of the ATN component of the AFTN/AMHS gateway, and an AU, as specified in Chapter 4. The AU is the message transfer and control unit of the AFTN/AMHS gateway.

2.2.1.4.2 For the support of the extended ATSMHS, an AFTN/AMHS gateway shall include a DUA as specified in 4.2.7.

2.2.2 AMHS information model

2.2.2.1 The following three categories of AMHS information objects shall be used:

- a) messages;
- b) probes; and
- c) reports.

2.2.2.2 *Messages.* In the basic ATSMHS, each AMHS message shall correspond unequivocally to an ATS message.

Note.— The provisions in Chapters §3 and §4 concerning ISO/IEC 10021 envelopes apply to transfer envelopes only.

2.2.2.3 *Probes.* Only direct AMHS users shall be able to submit AMHS probes.

2.2.2.4 *Reports.* AMHS reports shall be delivered only to direct AMHS users.

2.2.3 Security model

2.2.3.1 In the basic ATSMHS, security should be obtained by procedural means rather than by technical features inherent to the AMHS. In the basic ATSMHS, the security for each AMHS System is deemed a local issue to be addressed by the authority in charge of the system.

2.2.3.2 In the extended ATSMHS, a general AMHS security policy shall be implemented from ATS message user agent to ATS message user agent and provide the following security services:

- a) message origin authentication;

- b) content integrity; and
- c) message sequence integrity.

2.2.3.3 The general AMHS security policy aims to protect ATS message exchanges against the identified threats which are masquerade, modification and replay.

2.2.3.4 The general AMHS security policy is aligned with the general ATN security framework as defined in Part IV Chapter 3.

2.2.3.5 The general AMHS security policy is a common minimum which does not prevent specific communities of AMHS users from implementing more stringent security policies in case of additional user requirements.

2.2.3.6 The use of AMHS security services shall apply to:

- a) communications between direct AMHS users supporting the extended ATSMHS; and
- b) communications from direct AMHS users to AFTN/AMHS gateways supporting the extended ATSMHS.

2.2.3.7 The use of an asymmetric algorithm makes it possible to use security with indirect AMHS users in the direction from AMHS to AFTN only. Asymmetric signature mechanisms cannot be originated at an intermediate device such as a gateway.

2.2.3.8 The AMHS security policy shall make use of the ECDSA as specified in Part IV Chapter 3.

Note.— Part IV Chapter 3 is under development and this provision may need to be updated accordingly.

2.2.4 Management model

2.2.4.1 The scope of this manual for AMHS management is limited to the logging provisions which are defined for the ATS message user agent, the ATS message server and the AFTN/AMHS gateway. Storage, retrieval and exchange of any other management information is deemed a local issue to be addressed by the authority in charge of the system.

2.3 ORGANIZATION OF THE AMHS

2.3.1 The AMHS shall be organizationally composed of AMHS management domains.

2.3.2 An AMHS management domain may elect to operate as either an ADMD or a PRMD, depending on the national telecommunications regulation in force in the State(s) in which it operates and on its relationships with other management domains.

2.3.3 A PRMD which is subordinate to one or several AMHS ADMDs may qualify as AMHS management domain if it satisfies the provisions of this manual.

2.4 AMHS MANAGEMENT DOMAIN CONFIGURATIONS

2.4.1 Minimum set of systems

2.4.1.1 The minimum set of systems implemented and operated by an AMHS management domain shall be:

- a) an ATS message server and one or several ATS message user agents;
- b) an AFTN/AMHS gateway; or
- c) any combination of a) and b).

2.4.2 Interconnection between two AMHS management domains

2.4.2.1 An interconnection between two AMHS management domains shall be implemented as a connection between:

- a) two ATS message servers;
- b) an ATS message server and an AFTN/AMHS gateway; or
- c) two AFTN/AMHS gateways.

2.5 NAMING AND ADDRESSING PRINCIPLES

2.5.1 AMHS naming and addressing

2.5.1.1 AMHS O/R names

2.5.1.1.1 For the support of the basic ATSMHS, the O/R name of an AMHS user shall comprise:

- a) the O/R address of the AMHS user (called an MF-address); and
- b) optionally the directory name of the AMHS user, if the policy of the AMHS management domain, to which the AMHS user belongs, includes the local support of directory-names.

2.5.1.1.2 With regard to 2.5.1.1.1 b), as a matter of policy local to an AMHS management domain, the directory name component of an O/R name may be used by the implementation of the optional DIR FG.

2.5.1.1.3 For the support of the extended ATSMHS, the O/R name of an AMHS user shall comprise:

- a) the O/R address of the AMHS user (called an MF-address); and
- b) the directory name of the AMHS user.

2.5.1.2 Structure of an MF-address

The MF-address (MHS-form address) of an AMHS user shall comprise:

- a) a set of attributes, as specified in 2.5.1.3, identifying the AMHS management domain of which the AMHS user, either direct or indirect, is a service user; and
- b) a set of attributes, as specified in 2.5.1.4, uniquely identifying the AMHS user within the AMHS management domain, and in compliance with its declared addressing scheme. The attributes may include any standard or domain-defined attribute among those specified in ISO/IEC 10021-2, Section 18 other than *country-name*, *administration-domain-name* and *private-domain-name*.

2.5.1.3 AMHS management domain identifier

2.5.1.3.1 The attributes identifying an AMHS management domain shall include the following standard attributes as specified in ISO/IEC 10021-2, Section 18.3:

- a) *country-name*, taking the value “XX” as authorized by ITU-T to ICAO under the regime of Recommendation X.666 for international registered organizations,
- b) *administration-domain-name*, taking the value “ICAO” as registered by ITU-T for ICAO under the same regime,
- c) *private-domain-name*.

2.5.1.3.2 An AMHS management domain identifier shall be unique and declared to ICAO for insertion in the ICAO Register of AMHS Management Domains, by the State or organization in which the management domain operates.

2.5.1.3.3 The ICAO Register of AMHS Management Domains shall include at least one record, for each ICAO State, composed of the following attribute-values to be used in case no other AMHS management domain identifier has been declared by the State:

- a) *country-name*, taking the value “XX”,
- b) *administration-domain-name*, taking the value “ICAO”, and
- c) *private-domain-name*, taking one of the following values:
 - 1) the one or two nationality letters specified in Index to Nationality Letters for Location Indicators in Doc 7910 — *Location Indicators* if there is a one-to-one relationship between the nationality letters and the State;
 - 2) one of the pairs of nationality letters as specified in the Index in Doc 7910, uniquely allocated by the Secretariat if there are several pairs of nationality letters allocated to the State; or
 - 3) an ICAO designator composed of two to four letters, comprising the nationality letters and zero to two additional letters allocated by Secretariat to create a unique identifier.

2.5.1.3.4 To ensure the applicability of 2.5.1.3.3, *private-domain-name* values corresponding to nationality letters specified in Doc 7910 shall be reserved for potential use by an AMHS management domain operating in the State, or in one of the States, identified by the nationality letters.

2.5.1.3.5 The declaration of an AMHS management domain identifier shall:

- a) take precedence over the attribute-values specified in 2.5.1.3.3 provided that it does not contradict 2.5.1.3.4,
- b) cause overriding of the attribute-values specified in 2.5.1.3.3 by the declared attribute-values in the ICAO Register of AMHS Management Domains.

2.5.1.4 MF-addressing schemes

General provisions

2.5.1.4.1 It is a matter of policy local to an AMHS management domain to implement either an MF-addressing scheme, a locally defined AMHS addressing scheme or a combination of these. The two MF-addressing schemes defined in this manual are the common AMHS addressing scheme and the XF-addressing scheme. Additional MF-addressing schemes may be defined in the future.

2.5.1.4.2 Aeronautical industry X.400 addressing schemes are defined in appropriate aeronautical industry standards.

2.5.1.4.3 Each AMHS addressing scheme includes the set of attributes identifying the AMHS management domain as specified in 2.5.1.3.3.

2.5.1.4.4 An AMHS management domain should implement the common AMHS addressing scheme at the earliest opportunity to allocate MF-addresses to AMHS users within its domain of responsibility.

2.5.1.4.5 An AMHS management domain should avoid deviating from the common AMHS addressing scheme and refrain from implementing a locally defined AMHS addressing scheme unless specific unavoidable constraints (e.g. regulatory) apply to the AMHS management domain.

2.5.1.4.6 When an ICAO contracting State has not declared its use of the common AMHS addressing scheme, nor of a locally defined AMHS addressing scheme, then use of the XF-addressing scheme shall be assumed for indirect and direct AMHS users in this State.

XF-addressing scheme

2.5.1.4.7 An XF-address (translated-form address) is a particular MF-address of which the attributes identifying the user within an AMHS management domain (i.e. those attributes other than country-name, administration-domain-name and private-domain-name) may be converted by an algorithmic method to and from an AF-address (AFTN-form address). The algorithmic method requires the additional use of look-up tables which are limited, i.e. which include only a list of AMHS management domains rather than a list of individual users, to determine the full MF-address of the user.'

2.5.1.4.8 No distinction is made between upper case and lower case in an XF-address.

2.5.1.4.9 The XF-address of a direct or indirect AMHS user shall be composed exclusively of:

- a) an AMHS management domain identifier as specified in 2.5.1.3.3, composed of the attribute-values found for the State or organization of the user in the ICAO Register of AMHS Management Domains, using one of the following character combinations extracted from the user's AF-address, with an increasing order of preference from 1) to 3) in the case of multiple matches:

- 1) two-letters identifying a State as specified in Doc 7910 (characters 1 and 2 of the AF-address);

- 2) four-letters identifying a location as specified in Doc 7910 (characters 1 to 4 of the AF-address), and identifying a State if there is one single location in the State;
 - 3) a combination of either 1) or 2) above and a three-letter designator specified in *Designators for Aircraft Operating Agencies, Aeronautical Authorities and Services* (Doc 8585) identifying an organization within a State or at a location.
- b) an *organization-name* attribute:
- 1) as specified in ISO/IEC 10021-2, Section 18.3,
 - 2) taking the four-character value “AFTN”, and
 - 3) encoded as a printable string; and
- c) an *organizational-unit-names* attribute:
- 1) as specified in ISO/IEC 10021-2, Section 18.3,
 - 2) comprising a sequence of one single element, which takes the 8-character alphabetical value of the AF-address (AFTN-form address) of the user, and
 - 3) encoded as a printable string.

Common AMHS addressing scheme

2.5.1.4.10 The MF-address of a direct or indirect AMHS user complying with the common AMHS addressing scheme shall be composed exclusively of:

- a) an AMHS management domain identifier as specified in 2.5.1.3.3, composed of the attribute-values found for the State or organization of the user in the ICAO Register of AMHS Management Domains, using the following character combinations extracted from the user's AF-address, with an increasing order of preference from 1) to 3) in case of multiple matches:
 - 1) two-letters identifying a State as specified in Doc 7910 (characters 1 and 2 of the AF-address);
 - 2) four-letters identifying a location as specified in Doc 7910 (characters 1 to 4 of the AF-address), and identifying a State if there is one single location in the State;
 - 3) a combination of either 1) or 2) above and a three-letter designator specified in *Designators for Aircraft Operating Agencies, Aeronautical Authorities and Services* (Doc 8585) identifying an organization within a State or at a location; and
- b) an *organization-name* attribute specified in ISO/IEC 10021-2, Section 18.3 taking a value representing a geographical unit;
- c) an *organizational-unit-names* attribute specified in ISO/IEC 10021-2, Section 18.3 comprising a sequence of a single element which takes the four-character alphabetical value of the location indicator included in the AF-address of the user; and
- d) a *common-name* attribute specified in ISO/IEC 10021-2, Section 18.3 which takes the eight-character alphabetical value of the AF-address of the user.

2.5.1.4.11 No distinction is made between upper case and lower case in a MF-address complying with CAAS.

2.5.1.4.12 The *organization-name* attribute-values selected by an AMHS management domain shall be supplied to ICAO for publication in the ICAO Register of AMHS Management Domains, along with the ICAO location indicators included in the geographical unit represented by each *organization-name* attribute value.

2.5.1.5 AMHS naming schemes

For the support of the extended ATSMHS, the directory name of an AMHS user shall comply with the provisions of Part IV.

2.5.2 Upper layer naming and addressing

Application process titles

2.5.2.1 The application process title of an ATS message server should be as specified in Part III.

2.5.2.2 The application process title of an AFTN/AMHS gateway should be as specified Part III.

2.5.2.3 The application process title of an ATS message user agent should be as specified in Chapter 4 of Part III.

Application entity qualifiers

2.5.2.4 The application entity qualifier of an ATS message server should be “AMS” (integer value 7).

2.5.2.5 The application entity qualifier of an AFTN/AMHS gateway should be “GWB” (integer value 8).

2.5.2.6 The application entity qualifier of an ATS message user agent should be “AUA” (integer value 9).

Transport, session and presentation addresses

2.5.2.7 The TSAP of an ATS message server or of an ATS message user agent shall comply with the provisions of Part III.

2.5.2.8 The assignment of a transport selector value is a matter of policy local to an AMHS management domain.

2.5.2.9 The format and encoding of a session selector in the AMHS is specified in ISO/IEC ISP 11188-1, Section 9.3.

2.5.2.10 The assignment and administration of session selectors is a matter of policy local to an AMHS management domain.

2.5.2.11 The format and encoding of a presentation selector in the AMHS is specified in ISO/IEC ISP 11188-1, Section 7.2.

2.5.2.12 The assignment and administration of presentation selectors is a matter of policy local to an AMHS management domain.

2.6 AMHS ROUTING AND RE-ROUTING

2.6.1 The definition of AMHS routing shall be subject to multilateral agreement.

2.6.2 The MTA implemented by an AMHS management domain shall be collectively able to route on *country-name*, *ADMD-name*, *PRMD-name*, *organization-name* and *organizational-units-name* attributes.

2.7 AMHS TRAFFIC LOGGING UPON ORIGINATION

2.7.1 An AMHS management domain shall be responsible for long-term logging of all messages in their entirety which are originated by its direct AMHS users for a period of at least thirty days.

2.7.2 This requirement implies the logging of the entire BER-encoded ASN.1 messages.

Copyright International Civil Aviation Organization
Provided by IHS Markit under license with ICAO
No reproduction or networking permitted without license from IHS

Downloaded from ICAO Doc 9880 PART II 2016

Chapter 3

ATSMHS SPECIFICATION

3.1 ATS MESSAGE USER AGENT SPECIFICATION

3.1.1 Overview of the specification

3.1.1.1 For the support of the basic ATSMHS, an ATS message user agent complies with:

- a) the UA profile specified in 3.1.2, based on profile AMH21 as specified in ISO/IEC ISP 12062-2:1995 (1st or later Edition) and supporting the requirements of Repertoire Group A, for messages including a body part whose type is an extended body part type of general-text-body-part type; and
- b) the provisions related to traffic logging as specified in 3.1.3.

3.1.1.2 For the support of the extended ATSMHS, an ATS message user agent additionally complies with:

- a) the specifications in 3.1.4.2 which mandate the support of the IPM BC FG as specified in ISO/IEC ISP 12062-2:2003 (3rd Edition) and file-transfer body parts, in addition to the message content profile specification defined for the basic ATSMHS;
- b) the UA profile specified in 3.1.4.3, based on one of the following profiles, and depending on the inclusion of an MS in the attachment ATS message server and the application-contexts supported by the attachment ATS message server:
 - 1) AMH23 (MTS access – P3) as specified in ISO/IEC ISP 12062-4:2003;
 - 2) AMH25 (MTS 94 access – P3) as specified in ISO/IEC ISP 12062-4:2003;
 - 3) AMH24 (enhanced MS access – P7) as specified in ISO/IEC ISP 12062-5:2003; or
 - 4) AMH26 (enhanced MS 94 access – P7) as specified in ISO/IEC ISP 12062-6:2003;
- c) the DUA profile specified in 3.1.5.

3.1.2 UA profile specification in support of the basic ATSMHS

3.1.2.1 In the basic ATSMHS, there is no profile specification for the ATS message user agent at the level of the access protocol, i.e. at the level of the communication with the associated ATS message server, as this is considered to be a matter of policy local to each AMHS management domain. If it is desired to use standard ISO/IEC 10021 protocols for this communication, then profile AMH23 (for P3) or profile AMH24 (for P7) as specified in ISO/IEC ISP 12062-4:1995 (or a later edition) or ISO/IEC ISP 12062-5:1995 (or a later edition), respectively, may be implemented.

3.1.2.2 Message content profile specification

3.1.2.2.1 In an ATS message user agent, the content of the IPMs conveyed in support of the basic ATSMHS shall conform to the basic requirements of profile AMH21 as specified in Clause A.1 of ISO/IEC ISP 12062-2:1995 (or a later edition), Annex A and to the additional requirements described in Table 3-1 which are specific to the basic ATSMHS.

3.1.2.2.2 Table 3-1 specifies the additional requirements in the form of a PRL expressing restrictions to a set of rows of the profile AMH21, which are referred to using their reference in ISO/IEC ISP 12062-2. The specified requirements imply the use of interpersonal messaging as specified in 1988 version or later.

**Table 3-1. Requirements specific to the basic ATSMHS
in addition to profile AMH21**

Ref	Element	Origination		Reception		Basic ATSMHS support	Doc 9880 reference	ISP 12062-2 notes/ references
		Base	ISP	Base	ISP			
Part 1: AMH21/A.1.3 IPM body								
1	ia5-text	O	O	O	M	O/M		
1.2	data	M	M	M	M	M/M	3.3.3	
Part 2: AMH21/A.1.3.1 Extended body part support								
1	ia5-text-body-part	O	O	O	M	O/M		see AMH21/ A.1.3/1
11	general-text-body-part	O	M	O	M	M/M	3.3.3 and Part IV, Table 3-1	
Part 3: AMH21/A.1.5 Common data types								
1	RecipientSpecifier							
1.2	notification-requests	O	O	M	M	M/M	3.3.6	
1.2.1	rn	O	O	O	O	M/M	3.3.6	
1.2.2	nrm	O	O	M	M	M/M		
2	ORDescriptor							
2.1	formal-name	M	M1	M	M1	M1/M1	3.3.2	
Part 4: AMH21/A.1.3.2 General text repertoire support								
1	Basic (ISO 646) (repertoire identifiers {1, 6})	M	M	M	M	M/M		Repertoire Group A
2	Basic-1 (ISO 8859-1) (repertoire identifiers {1, 6, 100})	O	M	O	M	O/O		Repertoire Group B
M = mandatory support M1 = mandatory O/R name minimal support O = optional support								

3.1.2.3 Additional requirements for MT elements of service at an ATS message user agent

3.1.2.3.1 For the support of the basic ATSMHS, the *priority* element of an AMHS message generated at an ATS message user agent shall take the value “urgent” if, and only if, the value of the priority indicator in the ATS message priority as specified in 3.3.3.7.2 is “SS”.

3.1.2.3.2 For the support of the basic ATSMHS, the *priority* element of an AMHS message generated at an ATS message user agent shall take the value “urgent” only if it is ascertained that the MF-addresses identifying the message recipients do not specify a DL-name. Failure to meet this dynamic behaviour requirement may result in the absence of receipt-notification, even if the message has been properly delivered to the DL.

3.1.2.3.3 In the basic ATSMHS, the method for determining that an MF-address does not specify a DL-name is considered a local matter.

3.1.2.4 Interpretation of UTC time values

When generating and interpreting UTC time values, an ATS message user agent shall associate dates up to ten years prior to the current time and up to forty years ahead of the current time with the corresponding century, with the interpretation of the remaining 49 years being implementation dependent. This requirement is aligned with the convention used in ISO 10021-4:1997/Cor. 1:1998 and in ISO 10021-7:1997/Cor. 1:1998 for equivalent purposes.

3.1.3 Traffic logging requirements at an ATS message user agent

3.1.3.1 The requirement in 2.7 may be implemented in the ATS message user agent.

3.1.4 Additional UA profile specification in support of the extended ATSMHS

3.1.4.1 An ATS message user agent supporting the extended ATSMHS also needs to maintain the basic ATSMHS capability. Therefore the requirements in this section are in addition to those in 3.1.2.

3.1.4.2 Message content profile specification

3.1.4.2.1 An ATS message user agent supporting the extended ATSMHS shall conform to:

- a) the requirements of 3.1.2.2;
- b) the requirements additional to AMH21, described in Clause A.2.5 of ISO/IEC ISP 12062-2:2003 for the support of the IPM BC FG; and
- c) the additional requirements described in Table 3-2.

3.1.4.2.2 Table 3-2 specifies the additional requirements in the form of a PRL expressing restrictions to a set of rows of profile AMH21, which are referred to using their reference in ISO/IEC ISP 12062-2:2003.

3.1.4.2.3 The use of the bilaterally-defined body part as specified in Table 3-2/AMH21/A1.3.1 enables the exchange of unstructured binary data. In accordance with ISO/IEC 10021-7, 7.3.10 and the subsequent note, its use is now discouraged.

3.1.4.2.4 The use of the file-transfer body part as specified in Table 3-2/AMH21/A1.3.1 is the preferred means of conveying unstructured binary data in IPMs exchanged between ATS message user agents.

3.1.4.2.5 The requirements in 3.1.4.2.1 imply the use of interpersonal messaging as specified in the 1988 version or later.

**Table 3-2. Requirements specific to the extended ATSMHS
in addition to the basic ATSMHS**

Ref	Element	Origination		Reception		Extended ATSMHS support	Doc 9880 reference	ISP 12062-2 notes/ references
		Base	ISP	Base	ISP			
Part 1: AMH21/A.1.2 IPM heading fields								
17	extensions	M	M	M	M	M/M	3.3.4.1	
17.6	authorization-time	O	O	O	O	M/M	3.3.4.2	
17.12	originators-reference	O	O	O	O	M/M	3.3.4.3	
17.13	precedence-policy-identifier	O	O	O	O	M/M	3.3.4.5, 3.3.4.6 and 3.3.4.7	
Part 2: AMH21/A.1.3 IPM body								
10	bilaterally-defined	O	O	O	M	O/M	3.3.5	
Part 3: AMH21/A.1.3.1 Extended body part support								
9	bilaterally-defined-body-part	O	O	O	O	O/M	3.3.5.1	
12	file-transfer-body-part	O	O	O	O	M/M	3.3.5.1 and 3.3.5.2	AMH21/ A.1.3.3
Part 4: AMH21/A.1.5 common data types								
1	RecipientSpecifier							
1.4	recipient-extensions	O	M	O	M	M/M	3.3.4.1	
1.4.3	precedence	O	O	O	O	M/M	3.3.4.8	
M = mandatory support M1 = mandatory O/R name minimal support O = optional support								

3.1.4.2.6 For the encoding of a file-transfer-body-part, the octet-aligned EXTERNAL encoding shall be used as specified in ISO/IEC ISP 12062-2:2003. Only one EXTERNAL component shall be used. When the file to be conveyed contains a compound structure, this may be represented as a SEQUENCE OF EXTERNALS; the primary data shall be placed in the first EXTERNAL. Receiving systems may ignore all but the first EXTERNAL in the SEQUENCE.

3.1.4.3 Requirements for MT elements of service at an ATS message user agent

3.1.4.3.1 For the support of the extended ATSMHS, an ATS message user agent shall support one of the following, depending on the inclusion of an MS in the attachment ATS message server and the application-contexts supported by the attachment ATS message server:

- a) a profile based on profile AMH23 (MTS access – P3), as specified in ISO/IEC ISP 12062-4:2003, conforming to the:
 - 1) basic requirements of profile AMH23, as specified in Clause B.1 of the referenced ISP;

- 2) additional requirements described in Clause B.2.7 of the referenced ISP for support of the IPM SEC FG implementing Security-Class S0; and
- 3) additional requirements described in Clause B.2.8 of the referenced ISP for the support of the IPM DIR FG;
- b) a profile based on profile AMH25 (MTS 94 access – P3), as specified in ISO/IEC ISP 12062-4:2003, conforming to the:
 - 1) basic requirements of profile AMH25 as specified in Clause B.1 of the referenced ISP;
 - 2) additional requirements described in Clause B.2.7 of the referenced ISP for support of the IPM SEC FG implementing Security-Class S0; and
 - 3) additional requirements described in Clause B.2.8 of the referenced ISP for support of the IPM DIR FG;
- c) a profile based on profile AMH24 (enhanced MS access – P7) as specified in ISO/IEC ISP 12062-5:2003, conforming to the:
 - 1) basic requirements of profile AMH24 as specified in Clauses A.1 and B.1 of the referenced ISP for an MS-user;
 - 2) additional requirements described in Clause B.2.7 of the referenced ISP for support by an MS-user of the IPM SEC FG implementing Security-Class S0;
 - 3) additional requirements described in Clause B.2.8 of the referenced ISP for support by an MS-user of the IPM DIR FG; and
 - 4) the additional requirements described in Clause B.2.9 of the referenced ISP for support by an MS-user of the IPM BC FG; or
- d) a profile based on profile AMH26 (enhanced MS 94 access – P7) as specified in ISO/IEC ISP 12062-6:2003 conforming to the:
 - 1) basic requirements of profile AMH26 as specified in Clauses A.1 and B.1 of the referenced ISP for an MS-user;
 - 2) additional requirements described in Clause B.2.7 of the referenced ISP for support by an MS-user of the IPM SEC FG implementing Security-Class S0;
 - 3) additional requirements described in Clause B.2.8 of the referenced ISP for support by an MS-user of the IPM DIR FG; and
 - 4) the additional requirements described in Clause B.2.13 of the referenced ISP for the support by an MS-user of the IPM BC FG.

3.1.4.3.2 Due to the structure of ISO/IEC ISPs, 3.1.4.3.1 implicitly places requirements concerning the P3 or P7 implementation for the support of the:

- a) basic requirements of profiles AMH12, AMH13, AMH14 or AMH15 specified for common messaging in Annex A.1 of ISO/IEC ISPs 10611-4:2003, 10611-5:2003, 10611-4:2003 or 10611-6:2003, respectively;

- b) additional requirements specified for the common messaging SEC FG (implementing Security-Class S0) in Annex A.2 of these ISPs for an MTS-user or MS-user, as appropriate; and
- c) additional requirements specified for the common messaging DIR FG in Annex A.2 of these ISPs for an MTS-user or MS-user, as appropriate.

Security requirements

3.1.4.3.3 For the support of security in the context of the extended ATSMHS, an ATS message user agent shall make use of the ECDSA as specified in Part IV Chapter 3 for the signature algorithm.

Note.— Part IV Chapter 3 is under development and this provision may need to be updated accordingly.

3.1.4.3.4 For the generation of a secure AMHS message in compliance with the AMHS security policy defined in 2.2.3.2, an ATS message user agent supporting the extended ATSMHS shall include in the *per-recipient-extensions* of the message envelope, for each intended recipient, a message token:

- a) generated as specified in Table 3-3; and
- b) with a *criticality* field of the extension element taking the abstract-value “non-critical”.

3.1.4.3.5 Table 3-3 specifies the generation of the message token in the form of a PRL expressing requirements on both static support and dynamic use of the message token components. The rows, references and ISP requirements are extracted from the AMH12 – MTS access (P3) profile, as specified in ISO/IEC ISP 10611-4:2003. The specification applies identically if the ATS message user agent implements another P3 or P7 profile, since the message token description is common to all P3/P7 profiles.

3.1.4.3.6 In a secure AMHS message, the *token-type-identifier* element shall take the abstract-value “asymmetric-token”.

3.1.4.3.7 In a secure AMHS message, each *asymmetric-token* element shall be computed as specified in ISO/IEC 10021-4 by application of an ASN.1 SIGNED macro using DER as specified in ISO/IEC 9594-8/X.509, where the signature is generated by application of the ATN ASP specified in Part IV Chapter 3. There is no requirement to encode the full message using DER, but for the ASN.1 SIGNED and SIGNATURE macros, the use of encoding rules providing canonicity is mandated by X.509.

3.1.4.3.8 In a secure AMHS message, the *signature-algorithm-identifier* element of each *message-token* shall contain the algorithm OID value corresponding to the ATN signature scheme (“ecdsa-with-SHA1”), as specified in Part IV Chapter 3, and NULL parameters.

Note.— Part IV Chapter 3 is under development and the provisions above may need to be updated accordingly.

3.1.4.3.9 The *name* element of each *message-token* shall contain either the MF-address or the directory name of the intended recipient.

3.1.4.3.10 The *time* element of each *message-token* shall contain the time at which the message was generated.

3.1.4.3.11 The *content-integrity-check* extension element of each *message-token* shall contain:

- a) a digital signature applied to the concatenation of the OID value corresponding to the ATN signature scheme and the *message-content*; and

b) a *criticality* field of the extension element taking the abstract-value “non-critical”.

3.1.4.3.12 Upon reception of an AMHS message containing security elements, an ATS message user agent supporting the extended ATSMHS shall make use of a valid originator’s certificate to decode and verify the contained security elements by application of the ATN AVP specified in Part IV Chapter 3.

Note.— See note under 3.1.4.3.8.

3.1.4.3.13 The originator’s certificate may be obtained from the ATN directory, from the subject AMHS message itself if the originator included its certificate as a per-message-extension field of the message envelope, or from a local source.

3.1.4.3.14 The validity of the originator’s certificate may be checked using the mechanisms defined in Part IV which may include the use of ATN CRLs.

3.1.4.3.15 The verification of the digital signature may require DER re-encoding of the elements in clear which had been signed prior to the application of the hashing function for verification.

Table 3-3. Use of security elements (message token) in the extended ATSMHS

Ref	Element	Static support requirements			Dynamic action upon generation of a secure message	ATN reference
		Base	ISP (with support of SEC S0 FG)	Extended ATSMHS		
Part 1: AMH12/A.1.9/4 Extension data types (message token)						
4	MessageToken	O	M	M	G	
4.1	token-type-identifier	M	M	M	G	3.1.4.3.6
4.2	asymmetric-token	M	M	M	G	3.1.4.3.7
4.2.1	signature-algorithm-identifier	M	M	M	G	3.1.4.3.8
4.2.2	Name	M	M	M	G	3.1.4.3.9
4.2.3	Time	M	M	M	G	3.1.4.3.10
4.2.4	signed-data	O	M	M	G	↑
4.2.4.1	content-confidentiality-algorithm-identifier	O	C1	O	O	see Note
4.2.4.2	content-integrity-check	O	M	M	G	3.1.4.3.11
4.2.4.3	message-security-label	O	O	O	O	see Note
4.2.4.4	proof-of-delivery-request	O	O	O	O	see Note
4.2.4.5	message-sequence-number	O	O	O	O	see Note
4.2.5	encryption-algorithm-identifier	O	O	O	O	see Note
4.2.6	encrypted-data	O	O	O	O	see Note
4.2.6.1	content-confidentiality-key	O	O	O	O	see Note
4.2.6.2	content-integrity-check	M	M	M	O	see Note
4.2.6.3	message-security-label	O	O	O	O	see Note
4.2.6.4	content-integrity-key	O	O	O	O	see Note

Ref	Element	Static support requirements			Dynamic action upon generation of a secure message	ATN reference
		Base	ISP (with support of SEC S0 FG)	Extended ATSMHS		
4.2.6.5	message-sequence-number	O	O	O	O	see Note
C1 = if S0C then M else O G = generated M = mandatory support O = optional support <i>Note.— This element is not required as part of the AMHS security policy.</i>						

3.1.5 ATS message user agent DUA profile

3.1.5.1 For the support of the extended ATSMHS, an ATS message user agent shall include a DUA:

- a) supporting the DAP profile specified in Part IV; and
- b) supporting the DUA object classes and attribute types specified in Part IV.

3.1.5.2 The communication and interworking between the message handling service UA and the DUA included in an ATS message user agent are considered to be a local implementation matter, and as such they are not specified in this manual.

3.2 ATS MESSAGE SERVER SPECIFICATION

3.2.1 Overview of the specification

3.2.1.1 For the support of the basic ATSMHS, an ATS message server shall comply with:

- a) the profile specification expressed in 3.2.2; and
- b) the provisions related to traffic logging as specified in 3.2.3.

3.2.1.2 For the support of the extended ATSMHS, an ATS message server shall additionally comply with:

- a) one or several of the MTS-access and/or MS-access profiles specified in 3.2.4, based on the following profiles, depending on the inclusion of an MS in the ATS message server, and on the application-contexts supported by the ATS message server:
 - 1) AMH12 (MTS access – P3) as specified in ISO/IEC ISP 10611-4:2003;
 - 2) AMH14 (MTS 94 access – P3) as specified in ISO/IEC ISP 10611-4:2003;
 - 3) AMH13 (enhanced MS access – P7) as specified in ISO/IEC ISP 10611-5:2003; and
 - 4) AMH15 (enhanced MS 94 access – P7) as specified in ISO/IEC ISP 10611-6:2003.
- b) the DUA profile specified in 3.2.5.

3.2.2 Profile specification in support of the basic ATSMHS

3.2.2.1 P1 and upper layer requirements

3.2.2.1.1 In an ATS message server, the message transfer (P1) implementation of the IPM service in support of the basic ATSMHS shall conform to:

- a) the basic requirements of profile AMH22 as specified in Clause B.1 of ISO/IEC ISP 12062-3:1995, Annex B; and
- b) the additional requirements described in Clause B.2.2 for the support of the IPM DL FG.

3.2.2.1.2 The specification in 3.2.2.1 implicitly places the following requirements on the P1 implementation:

- a) the basic requirements of profile AMH11 specified for common messaging in Annex A.1 of ISO/IEC ISP 10611-3:1994 implying mandatory support of profile AMH111 implementing the MTS-transfer application context; and
- b) the additional requirements specified for the common messaging DL FG in Annex A.2.2 of ISO/IEC ISP 10611-3:1994.

3.2.2.1.3 As a consequence of 3.2.1.2, the optional implementation of MS in an ATS message server, being related to the access protocol from an ATS message user agent to an ATS message server, is a matter of policy local to an AMHS management domain.

3.2.2.1.4 The additional support by an ATS message server of profile AMH112 as specified in ISO/IEC ISP 10611-3:1994 for conformance to CCITT X.400, in order to interconnect with public ADMDs, is a matter of policy local to an AMHS management domain.

3.2.2.1.5 For the use of the ACSE by an AMHS application, the application-context name which is used as a parameter in an A-ASSOCIATE is defined in the base standards (see ISO/IEC 10021-6).

3.2.2.1.6 The specification in 3.2.2.1 places no requirements of the RTSE or ACSE other than conformance with ISO/IEC ISP 10611-2:1994 in accordance with the P1 application-context(s) for which conformance is claimed.

3.2.2.1.7 The specification in 3.2.2.1 places no requirements on the presentation and session layers other than conformance with ISO/IEC ISP 10611-2:1994 in accordance with the P1 application-context(s) for which conformance is claimed.

3.2.2.2 Use of the transport service

3.2.2.2.1 The basic ATSMHS shall make use of the connection mode transport service in either or both of the following configurations:

- a) provided by the ATN ICS as generally specified in Part III with the additional specifications in 3.2.2.2.3 to 3.2.2.2.6; or
- b) provided by the IPS as generally specified Doc 9896, with the additional specifications in 3.2.2.2.7, 3.2.2.2.8 and 3.2.2.2.9.

3.2.2.2.2 For the support of the basic ATSMHS, the use of the expedited data option at the establishment of the transport connection is a local matter which may depend on the implemented application-context.

Transport service over the ATN ICS

3.2.2.2.3 For the support of the basic ATSMHS over the ATN ICS, the connection mode transport service provided by the ATN COTP as specified in Part III shall be used.

3.2.2.2.4 For the support of the basic ATSMHS, transport connections shall be established over the ATN transport service between systems belonging to the AMHS using the RER abstract-value “high”.

3.2.2.2.5 For the support of the basic ATSMHS, transport connections shall be established over the ATN transport service between systems belonging to the AMHS using the transport connection priority abstract-value “6” which corresponds to the message category “flight regularity communications”.

3.2.2.2.6 For the support of the basic ATSMHS, transport connections shall be established over the ATN transport service between systems belonging to the AMHS using the value of the ATN security label as specified in Part III which corresponds to:

- a) the ATN traffic type “ATN operational communications”;
- b) the subtype “air traffic services communications”; and
- c) “no traffic type policy preference”.

Transport service over the ATN IPS

3.2.2.2.7 For the support of the basic ATSMHS over the ATN IPS, the connection mode transport service provided by the IPS TCP shall be used.

3.2.2.2.8 When the IPv4 protocol version is used, the connection mode transport service over TCP shall be provided as specified in RFC1006.

3.2.2.2.9 When the IPv6 protocol version is used, the connection mode transport service over TCP shall be provided as specified in RFC2126.

3.2.2.3 Interpretation of UTC time values

When generating and interpreting UTC time values, an ATS message server shall associate dates up to ten years prior to the current time and up to forty years ahead of the current time with the corresponding century, with the interpretation of the remaining forty-nine years being implementation dependent. This requirement is aligned with the convention used in ISO 10021-4:1997/Cor. 1:1998 for equivalent purposes.

3.2.3 Traffic logging requirements at an ATS message server

3.2.3.1 The ATS message server shall perform a long-term logging, for a period of at least thirty days, of the actions taken with respect to every message received at the ATS message server, whether from an ATS message user agent or from another ATS message server, and to every report received or generated at the ATS message server.

3.2.3.2 For the long-term logging of information related to a message submitted to or received by an ATS message server, the following parameters related to the message shall be logged:

- a) *message-identifier*;
- b) *priority*;
- c) *content-type*;
- d) *originator-name*;
- e) *recipient-name* elements on responsibility list, which identify recipients whose *per-Recipient-Indicator responsibility* bit has the abstract-value “responsible”;
- f) *message-content-size*;
- g) last element of the *trace-information* (if any);
- h) *arrival-time* or *submission-time*;
- i) transfer destination (if any);
- j) transfer time (if any);
- k) *this-recipient-name* (if message delivery is performed by the ATS message server);
- l) *delivery-time* (if any);
- m) delivery and/or non-delivery reports generated (if any); and
- n) event date/time.

3.2.3.3 For the long-term logging of information related to a report generated or received by an ATS message server, the following parameters related to the report shall be logged:

- a) *report-identifier*;
- b) *subject-identifier*;
- c) *actual-recipient-name* elements;
- d) *report-type* elements;
- e) *report-destination-name*;
- f) last element of the *trace-information* (if any);
- g) *arrival-time* in the ATS message server or generation time;
- h) transfer destination (if any);
- i) transfer time (if any);
- j) *OR-name* of the report recipient (if report delivery is performed by the ATS message server);
- k) *delivery-time* (if any); and