AFI AMHS Manual

Appendix B

European ATS Messaging Service Profile	
Document Reference:	EUR AMHS Manual, Appendix B
Author:	ICAO AFSG PG
Revision Number:	Version 2.0
Date:	27/07/2013
Filename:	AFI_AMHS_Manual-Appx_B-v2.0.doc

Document Control Log

Edition	Date	Comments	section/pages affected
1.0	28/07/2011	Created from AFI AMHS Manual, version 6.1 Appendix A, B, and C	All
2.0	28/07/2013	Created from EUR AMHS Manual, version 8.0	All

Table of contents

References

[1] Internet Engineer Task Force (IETF) STD0007, RFC0793:1981, Transmission Control Protocol

[2] Internet Engineer Task Force (IETF) STD0005, RFC0791:1981, Internet Protocol

[3] Internet Engineer Task Force (IETF) STD0003, RFC1122:1989, Requirements for Internet Hosts - Communication Layers

[4] Internet Engineer Task Force (IETF) RFC4301:2005, Security Architecture for the Internet Protocol (IPsec)

[5] Internet Engineer Task Force (IETF) RFC2460:1998, Internet Protocol, Version 6 (IPv6) Specification

[6] Internet Engineer Task Force (IETF) RFC4443:2006, Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification

[7] Internet Engineer Task Force (IETF) BCP0028, RFC2488:1999, Enhancing TCP over Satellite Channels Using Standard Mechanisms

[8] ISO/IEC 7498-1:1994 (2nd edition), Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model

[9] ICAO Annex 10 – Aeronautical Telecommunications, Volume III

[10] ICAO 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), First Edition – 2010

[11] ICAO Doc 9880-AN/466: Manual on Detailed Technical Specifications for the Aeronautical Telecommunication Network (ATN) using ISO/OSI Standards and Protocols, Part III – Upper Layer Communications Service (ULCS) and Internet Communications Service (ICS), , First Edition – 2010

[12] ICAO Doc 9880-AN/466: Manual on Detailed Technical Specifications for the Aeronautical Telecommunication Network (ATN) using ISO/OSI Standards and Protocols, Part IV – Directory Services, Security and Systems Management, First Edition – 2010

[13] CCITT Rec X.400 (1992). Message handling system and service overview

[14] CCITT Rec X.402 (1992). Message handling systems: overall architecture

[15] CCITT Rec X.411 (1992). Message handling systems: Message transfer system: Abstract service definition and procedures

[16] CCITT Rec X.419 (1992). Message handling systems: Protocol specifications

[17] CCITT Rec X.420 (1992). Message handling systems: Interpersonal messaging system

[18] ISO/IEC 646:1991. Information technology — ISO 7-bit coded character set for information interchange

[19] ISO/IEC 3166:1993. Codes for the representation of names and countries

[20] ISO/IEC 8859-1: 1987. Information processing — 8-bit single-byte coded graphics character sets — Part 1: Latin alphabet No. 1

[21] ISO/IEC TR 10000-1: 1995. Information technology — Framework and taxonomy of International Standardized Profiles — Part 1: General principles and documentation framework

[22] ISO/IEC TR 10000-2: 1995. Information technology — Framework and taxonomy of International Standardized Profiles — Part 2: Principles and taxonomy for OSI profiles

[23] ISO/IEC 10021-1:1990. Information Technology — Text Communication — Message-Oriented Text Interchange System (MOTIS) — Part 1: System and Service Overview

[24] ISO/IEC 10021-1/Amd.2:1994. Information Technology — Text Communication — Message-Oriented Text Interchange System (MOTIS) — Part 1: System and Service Overview

[25] ISO/IEC 10021-2:1990. Information Technology — Text Communication — Message-Oriented Text Interchange System (MOTIS) — Part 2: Overall Architecture

[26] ISO/IEC 10021-2/Amd.1:1993. Information Technology — Text Communication — Message-Oriented Text Interchange System (MOTIS) — Part 2: Overall Architecture

[27] ISO/IEC 10021-2/Amd.2:1994. Information Technology — Text Communication — Message-Oriented Text Interchange System (MOTIS) — Part 2: Overall Architecture

[28] ISO/IEC 10021-3:1990. Information Technology — Text Communication — Message-Oriented Text Interchange System (MOTIS) — Part 3: Abstract Service Definition Conventions

[29] ISO/IEC 10021-4:1990. Information Technology — Text Communication — Message-Oriented Text Interchange System (MOTIS) — Part 4: Message Transfer System: Abstract Service Definition and Procedures

[30] ISO/IEC 10021-4/Amd.1:1994. Information Technology — Text Communication — Message-Oriented Text Interchange System (MOTIS) — Part 4: Message Transfer System: Abstract Service Definition and Procedures

[31] ISO/IEC 10021-5:1990. Information Technology — Text Communication — Message-Oriented Text Interchange System (MOTIS) — Part 5: Message Store: Abstract Service Definition

[32] ISO/IEC 10021-5/Amd. 1:199x. Information Technology — Text Communication — Message-Oriented Text Interchange System (MOTIS) — Part 5: Message Store: Abstract Service Definition

[33] ISO/IEC 10021-6:1990. Information Technology — Text Communication — Message-Oriented Text Interchange System (MOTIS) — Part 6: Protocol Specifications

[34] ISO/IEC 10021-7:1990. Information Technology — Text Communication — Message-Oriented Text Interchange System (MOTIS) — Part 7: Interpersonal Messaging System

[35] ISO/IEC ISP 10611-1:1994. Information Technology — International Standardized Profiles AMH1n — Message Handling Systems — Common Messaging — Part 1: MHS Service Support

[36] ISO/IEC ISP 10611-2:1994. Information Technology — International Standardized Profiles AMH1n — Message Handling Systems — Common Messaging — Part 2: Specification of ROSE, RTSE, ACSE, Presentation and Session Protocols for use by MHS

[37] ISO/IEC ISP 10611-3:1994. Information Technology — International Standardized Profiles AMH1n — Message Handling Systems — Common Messaging — Part 3: AMH11-Message Transfer (P1)

[38] ISO/IEC ISP 10611-4:1994. Information Technology — International Standardized Profiles AMH1n — Message Handling Systems — Common Messaging — Part 4: AMH12-MTS Access (P3)

[39] ISO/IEC ISP 10611-5:1994. Information Technology — International Standardized Profiles AMH1n — Message Handling Systems — Common Messaging — Part 5: AMH13-MS Access (P7)

[40] ISO/IEC ISP 11188-1:1995. Information Technology — International Standardized Profile — Common Upper Layer Requirements — Part 1: Basic connection oriented requirements

[41] ISO/IEC ISP 12062-1:1995. Information Technology — International Standardized Profiles AMH2n — Message Handling Systems — Interpersonal Messaging — Part 1: IPM MHS Service Support

[42] ISO/IEC ISP 12062-2:1995. Information Technology — International Standardized Profiles AMH2n — Message Handling Systems — Interpersonal Messaging — Part 2: AMH21 — IPM Content

[43] ISO/IEC ISP 12062-3:1995. Information Technology — International Standardized Profiles AMH2n — Message Handling Systems — Interpersonal Messaging — Part 3: AMH22 — IPM Requirements for Message Transfer (P1)

[44] ISO/IEC ISP 12062-4:1995. Information Technology — International Standardized Profiles AMH2n — Message Handling Systems — Interpersonal Messaging — Part 4: AMH23 — IPM Requirements for MTS Access (P3)

[45] ISO/IEC ISP 12062-5:1995. Information Technology — International Standardized Profiles AMH2n — Message Handling Systems — Interpersonal Messaging — Part 5: AMH24 — IPM Requirements for MS Access (P7)

[46] ISO/IEC 10021-1:2003. Information Technology — Text Communication — Message Handling Systems (MHS) — Part 1 : System and Service Overview

[47] ISO/IEC 10021-2:2003. Information Technology — Text Communication — Message Handling Systems (MHS) — Part 2: Overall Architecture

[48] ISO/IEC 10021-4:2003. Information Technology — Text Communication — Message Handling Systems (MHS) — Part 4: Message Transfer System: Abstract Service Definition and Procedures

[49] ISO/IEC 10021-5:1999. Information Technology — Text Communication — Message Handling Systems (MHS) — Part 5: Message Store: Abstract Service Definition

[50] ISO/IEC 10021-6:2003. Information Technology — Text Communication — Message Handling Systems (MHS) — Part 6: Protocol Specifications

[51] ISO/IEC 10021-7:2003. Information Technology — Text Communication — Message Handling Systems (MHS) — Part 7: Interpersonal Messaging System

[52] ISO/IEC ISP 10611-4:2003. Information Technology — International Standardized Profiles AMH1n — Message Handling Systems — Common Messaging — Part 4: AMH12 and AMH14 - MTS Access (P3) and MTS 94 Access (P3). (Edition 3)

[53] ISO/IEC ISP 10611-5: 2003. Information Technology — International Standardized Profiles AMH1n — Message Handling Systems — Common Messaging — Part 5: AMH13-MS Access (P7). (Edition 3)

[54] ISO/IEC ISP 10611-6: 2003. Information Technology — International Standardized Profiles AMH1n — Message Handling Systems — Common Messaging — Part 5: AMH15-MS 94 Access (P7). (Edition 2)

[55] ISO/IEC ISP 12062-1: 2003. Information Technology — International Standardized Profiles AMH2n — Message Handling Systems — Interpersonal Messaging — Part 1: IPM MHS Service Support (Edition 3)

[56] ISO/IEC ISP 12062-2: 2003. Information Technology — International Standardized Profiles AMH2n — Message Handling Systems — Interpersonal Messaging — Part 2: AMH21 — IPM Content (Edition 3)

[57] ISO/IEC ISP 12062-3: 2003. Information Technology — International Standardized Profiles AMH2n — Message Handling Systems — Interpersonal Messaging — Part 3: AMH22 — IPM Requirements for Message Transfer (P1). (Edition 3)

[58] ISO/IEC ISP 12062-4: 2003. Information Technology — International Standardized Profiles AMH2n — Message Handling Systems — Interpersonal Messaging — Part 4: AMH23 and AMH25 — IPM Requirements for MTS Access (P3) and MTS 94 Access (P3). (Edition 3)

[59] ISO/IEC ISP 12062-5: 2003. Information Technology — International Standardized Profiles AMH2n — Message Handling Systems — Interpersonal Messaging — Part 5: AMH24 — IPM Requirements for Enhanced MS Access (P7). (Edition 3)

[60] ISO/IEC ISP 12062-6: 2003. Information Technology — International Standardized Profiles AMH2n — Message Handling Systems — Interpersonal Messaging — Part 6: AMH26 — IPM Requirements for Enhanced MS 94 Access (P7). (Edition 2)

[61] IETF STD0035 RFC 1006:1987 – ISO Transport Service on top of TCP (TP-TCP)

[62] IETF RFC 2126:1997 – ISO Transport Service on top of TCP (ITOT)

[63] EUR Doc 020, EUR AMHS Manual, Appendix A "Abbreviations, Glossary and Definitions", latest version

[64] ICAO Doc 9896-AN/469: Manual on the Aeronautical Telecommunication Network (ATN) using Internet Protocol Suite (IPS) Standards and Protocols, First Edition – 2010

Table of Figures

List of Tables

1. Introduction

1.1 Purpose of the Document

The following documents and standards contain provisions which, through reference in this text, constitute provisions of this Profile.

At the time of publication of this Profile, the editions indicated for the referenced documents and standards were valid.

Revisions of the referenced documents shall not form part of the provisions of this Profile until they are formally reviewed and incorporated into this Profile.

In case of conflict between the requirements of this Profile and the contents of the referenced documents, this Profile shall take precedence.

1.2 Referencing the ISP 1st, 2nd and 3rd Editions

Doc 9880, Part II [10] refers to Edition 1 of the ISPs to define the Basic ATS Message Handling Service, and it refers to Edition 3 ISPs to define the Extended ATS Message Handling Service. Edition 2 ISPs are not referenced.

This situation complicates the specification of this Profile, because it references both the Basic and Extended ATS Message Handling Services. The Basic Service definitions in Doc 9880, Part II [10] should be updated to refer exclusively to Edition 3 ISPs – thus eliminating all references to Edition 1 ISPs.

In the meantime, this Profile, and the profiling tables in its Annexes all refer to the elements of the 3rd Edition ISPs. Annex R provides a mapping between the elements of Edition 3 to the corresponding elements of Edition 1 ISPs.

2. Definitions

For the purpose of this Profile, the following definitions shall apply:

Profile: A set of one or more base standards, and, where applicable, the identification of chosen classes, subsets, options and parameters of those base standards, necessary for accomplishing a particular function.

Profile Requirements List (PRL): The profile requirements are expressed in the form of conformance requirements and are arranged in a tabular list format.

Protocol Implementation Conformance Statement (PICS): A statement made by the supplier of a system, stating which capabilities have been implemented for a given protocol.

Implementation: a conforming AMHS implementation of this Profile which is uniquely defined by its IP address, TCP port and, if applicable, its associated OSI TSAP, SSAP PSAP and Application Entity Title.

3. Technical Overview

3.1 ATS Message Handling Service Support

The ATS Message Handling System includes several types of system:

ATS Message User Agents – ATS Message Servers are accessed remotely using an ATS Message User Agent. Therefore each individual user or group of users at a physical location that require access to AMHS must be provided with an ATS Message User Agent.

The user may be a person or some type of system that automatically generates and/or receives messages.

ATS Message User Agents generate, and must accept the contents of messages and Message Envelopes transmitted between International COM centres. Some of the provisions of this Profile therefore apply to ATS Message User Agents. Some other purely local aspects of the protocols used to connect a UA to an MTA or MS will need to be specified separately by the ANSP to suit their own requirements.

ATS Message Servers – these provide the Message Transfer Service and perform the entire common message processing for a number of attached ATS Message User Agents. They support ATS Message User Agents and Message Stores access to the server for message Submission and Delivery, and interchange messages with other ATS Message Servers in other locations.

An ATS Message Server supporting AMHS contains an MTA. Some of the provisions of this Profile therefore apply to the MTA components used in AMHS systems.

An ATS Message server may also contain a Message Store. Message Stores are required to be effectively transparent to international message interchange, and therefore are not subject to the provisions of this Profile. However, they will be the subject of local specifications by the ANSP procuring an MS.

The AMHS may also include a further component such as AFTN/AMHS Gateway, however, this is out of the scope of this Profile.

3.2 ATS-Message Handling System components

ATS Message Servers and ATS Message User Agents are supported by the MHS system components outlined in the following sections.

3.2.1 ATS-Message User Agent components

Each ATS Message User Agent consists of an MHS User Agent, possibly a Directory User Agent (DUA) and some form of user interface.

User Agent (UA) – The task of a UA is to provide one or more users at a particular location with remote access to Message Handling Services provided by the MTA. In

particular, they support the users to create and receive Inter-Personal Messages formatted to ATS requirements.

Directory User Agent (DUA) – The task of a Directory User Agent is to provide one or more users at a particular location with access to a Directory Service Agent to allow the users to determine other user's OR-Addresses and messaging capabilities. The DUA is not profiled in this document.

3.2.2 ATS Message Servers

ATS Message Servers consist of a Message Transfer Agent and optionally an access point for Message Transfer Service access, a Message Store, and may include a Directory User Agent:

Message Transfer Agent (MTA) – The task of an MTA component is to provide the Message Handling Services to users, and in particular, to transfer messages directly or indirectly to users attached to other Message Transfer Agents using Store and Forward messaging techniques. Each international COM Centre that supports AMHS must communicate with other international COM Centres using an MTA.

Message Store (MS) – The task of a Message Store is to take delivery of messages on behalf of a User Agent and hold them until the user retrieves them through the UA.

MTS Access for remote MTS Users – This provides an access point to the Message Transfer Agent for MTS users (e.g. either Remote UAs and/or Message Stores).

Directory User Agent (DUA) – The task of a DUA is to provide the MTA with access to a Directory Service Agent (which holds directory information) to allow the determination of user OR-Addresses and user's messaging capabilities, to provide AMHS<>AFTN Address mapping information, and to hold AMHS Security and Distribution List details. The DUA is not profiled in this Profile.

Co-located MHS User Agents (UA) – Some Message Server configurations may include a Co-located User Agent that supports remote access for the user's system/terminal using some proprietary protocol (e.g. via a proprietary LAN solution).

3.3 AMHS and other Protocols

The AMHS system components outlined above communicate with each other using standard protocols specified in the Message Handling Systems Base Standards, the International Standardized Profiles (ISPs), Doc 9880, Part II [10] and some Internet RFCs. The following subsections give an overview:

3.3.1 The IPM Content Type

The ATS Message Handling Service is based on the Inter-Personal Messaging Content Type. This is a Profile that specifies the form and fields of an IPM message Heading and Body Parts. The IPM Content Type is used by UAs that generate AMHS IP Messages, and by UAs that receive AMHS IP Messages. The protocol (referred to as P2) is therefore used in communications between IPM-conformant User Agents. The IPM content Type is profiled by Doc 9880, Part II [10] to support the ATS Message Handling Service.

3.3.2 AMHS Body Part Types

In the ATS Messaging Service, an IPM shall contain either:

a) a single IA5-text body part in support of textual data exchange, or

b) a single general-text body part in support of textual data exchange, or

c) a single file-transfer body part in support of binary data exchange.

Use of the bilaterally-defined body part (as specified in earlier editions of former Doc 9705) is deprecated.

3.3.3 Message Transfer – P1

ATS Messages are transferred between MTA components of ATS Message Servers using a Message Store-and-Forward Protocol referred to as P1. There are a number of different specifications of P1, each suited to a particular situation. One of these is mandated in this Profile. Each ATS message will be transferred between MTAs in a Message Envelope that conforms to the P1 Protocol.

3.3.4 Message Transfer System Access – P3

ATS Messages are transferred between MTS-Users (UAs and MSs) and MTAs during message Submission and Delivery using a protocol referred to as P3. The ISPs, together with this Profile mandate facilities for users to be able to construct valid AMHS message IPM-Headings, IPM Body Parts, MTS Envelopes and valid AMHS Addresses (OR-Addresses) by using standard MHS Elements of Service.

This form of MTS access is referred to as ‘forced access’ because messages arriving at the MTA are immediately ‘force’ delivered to the UA (as opposed to being stored in a Message Store). This is an important consideration for users that may receive urgent, high priority messages (e.g. ‘SS’ priority ATS messages).

However, it should be noted that the P3 protocol is not often used in commercial environments because commercial users generally prefer to use Message Store Access (P7) which more adequately suits their needs. This means that P3 based UAs and MTAs might not be quite so readily available in the marketplace.

3.3.5 Proprietary MTS Access

If an ATC application (e.g. Flight Planning System) and its UA are co-located with an MTA on a common hardware platform, then the Application Program Interface between the UA and MTA supports the MT-Access Abstract Service as defined for P3.

3.3.6 Proprietary MTS Access (Co-Located UA)

In some configurations a UA may be co-located with the MTA on the same platform. In these cases, the UA and MTA exchange messages over a systems internal Application Programming Interface (using the P3 Abstract Service), and the UA is accessed from the remote user’s site using a local system (e.g. a non-P3 Personal Computer). The remote system and the UA component communicate using some proprietary protocols (e.g. via a LAN or using a dial-up connection).

In these cases, it is important to ensure that the remote user's system can access all of the necessary facilities and MHS Elements of Service to construct, submit and take delivery of valid ATS message IPM-Headings, IPM Body Parts, MTS Envelopes and valid AMHS Addresses (OR-Addresses).

3.3.7 Message Store Access – P7

Some users may optionally be configured with a Message Store that is attached permanently to the MTA to take message delivery. Users access the Message Store and retrieve delivered messages at their own convenience. The protocol used for communications between the UA and the MS is referred to as P7.

Messages are not 'force-delivered' to users of Message Stores, so, Message Stores should not be configured for users who might receive urgent, high priority messages (e.g. 'SS' priority ATS messages) unless the Message Store is locally configured with an appropriate function called the "Alert Auto-Action".

Message Stores are often co-located with their MTA, and an Application Programming Interface (API) is used for communications between MTA and MS. This API supports the MT-Access Abstract Service (P3).

In other, rare, cases an MS may be remote from the MTA, in which case the P3 protocol is used for Message Submission and Delivery between the MS and MTA.

3.3.8 Message Store Access P7 (94)

In 1994, an upgraded Message Store was defined in the MHS Base Standards (referred to as MS (94) P7). For the purposes of ATS Messaging in the context of this Profile, there is no distinction between the MS and MS(94) systems, since all of the base standards enhancements of the MS(94) systems are of a purely local nature (i.e. effective only between the UA and the MS and not effective on an end-to-end basis). The enhancements allow the user to create and store draft messages in the message store. It also includes more Auto Action types, and enables enhanced message manipulation. Procurers may need to become aware of these distinctions and specify the local options of the MS that are appropriate to the MS user's intended task.

3.3.9 Proprietary Message Store Access

In some configurations, a UA may be partly co-located with the MS. In these cases, the UA and MS exchange messages over a systems internal Application Process Interface, and the UA is accessed from the remote user's site using a local system (e.g. a non-P7 Personal Computer). The remote system and the UA component communicate using some proprietary protocols (e.g. via a LAN or using a dial-up connection). In these cases, it is important to ensure that the remote user's system can access all of the necessary facilities and MHS Elements of Service to construct and retrieve valid AMHS message IPM-Headings, IPM Body Parts, MTS Envelopes and valid AMHS Addresses (OR-Addresses).

3.3.10 Upper Layer Support

The Upper Layers of OSI are used to support communications between MTAs, UAs and MSs. The protocols involved are the ROSE, RTSE, ACSE, Presentation and Session protocols. The use of OSI upper layers is specified as a common ISP for all of the MHS Applications (MTA, UA and MS). These rely on provision of an OSI Transport Service.

3.3.11 Transport

The Upper Layers use a common set of OSI Transport Services. However, the OSI Transport Layer Protocols are not used in the EUR AMHS Profile. Instead the OSI Transport Service is supported by RFCs 1006 and 2126 as a means of utilising an underlying TCP/IP data communications service.

3.3.12 Lower Layers and TCP/IP

This Profile specifies the use of TCP/IP for interconnections between MTAs of different ANSP International COM Centres within Europe. The same Lower Layer profile may also be used within ANSP's local systems – e.g. to support P1, P3 and P7.

Additional protocol stacks may be required in other situations (e.g. the ATN profile may be additionally required to connect to other inter-Regional gateways, and other profiles may need to be used between the MTAs operating within an ANSP's Management Domain).

3.4 Common Facilities

3.4.1 Directory Access

The EUR AMHS Profile indicates information that may be obtained from the Directory by ATS User Agents and ATS Message Servers. A number of technical options exist for accessing the Directory information. In most cases the ANSP provider will select one of the options locally for use within the ANSP. Therefore, the protocol profile for Directory Access is not specified in this Profile.

3.4.2 Directory Schema

The X.500 Base Standards together with their respective ISPs specify a common directory schema of Object Classes, Attribute Types and Attribute Syntaxes that form a foundation schema for all Directories.

ISO/IEC 10021 - 2 specifies a further set of Object Classes and Attribute Types and Attribute Syntaxes for the support of the MHS Use of the Directory Functional Group.

Part IV of Doc 9880 [12] augments these definitions to include further Object Classes and Attributes Types that are to be used within the ATC community (the ATN Directory). In particular, a set of ATN Object Classes and Attribute Types have been specified for use with AMHS supporting the Extended ATS Message Handling Service.

The EUR AMHS Profile indicates the Directory Information that should be available to AMHS systems in terms of these schema elements in Annex K but does not mandate that the Directory is accessed to obtain it.

3.4.3 Cryptographic profile

The Extended ATS Messaging Service requires the support of the S0 Functional Group, which applies to the various forms of User Agent. However, the ISPs do not specify the cryptographic parameters (e.g. cryptographic algorithms and parameters) to be used. These are specified by Doc 9880, Part IV [12] for AMHS, and furthermore over time, they are liable to change. The cryptographic profile provided by this Profile contains references to those further

specifications of cryptography algorithms and value settings of individual protocols fields necessary to secure ATS messages.

Note. – The S0 functional group is not specified by the EUR AMHS Profile.

Note. – The Cryptographic profile has been treated in a separate Annex for simplicity of maintenance, and the fact that it is referenced by a number of different AMHS component types.

3.5 Addressing and Address Registration

AMHS Systems use Originator-Recipient Addresses (OR-Addresses) to identify and locate users within the MTS. Doc 9880, Part II [10] specifies a number of OR-Address Forms for use in AMHS.

Doc 9880, Part II [10] also specifies and registers appropriate address values for use with the OSI upper layer addressing.

The RFCs specify 'well-known' TCP-port identifiers for use with RFC 1006/2126 applications.

This Profile collects these values in a Register of Address Values in Annex N.

3.6 ANSP's AMHS System local configurations

ANSPs will need to configure their own AMHS systems according to local requirements. Accordingly, the specifications of this Profile constrain only those aspects that are necessary to guarantee Regional (EUR) interchange of ATS messages.

However, this does mean that ANSPs will need to define their own systems local configurations (such as location of UAs, MTAs, and their interconnectivity etc.) and they may need to provide further specifications for any purely local protocol aspects that remain options in the ISPs on which this Profile is based (e.g. options for Message Retrieval from Message Stores, and the details of UA/MTA and UA MS Bind Operations and Authentication resulting from an ANSP's local security policy).

3.7 Protocol Stacks

The following illustrates the different applications profiled in this Profile together with their underlying protocol stacks.

Ref	Layer	UA	MS	MTA
1	Application	P3 + IPM	P7 or P7 (94) + IPM	P1 + IPM
2	ROSE	Y	Y	-
3	RTSE	O	O	Y

Ref	Layer	UA	MS	MTA
4	ACSE	Y		
5	Presentation	Y		
6	Session	Y		
7	Transport	Y (RFC 1006 or 2126 over TCP)		
8	Network	Y (IPv6 or IPv4)		

Table 3.7.1: AFI AMHS Protocol Stacks

Y = Layer protocol implemented
O = Optionally implemented
- = Not used

4. AFI AMHS Profile Requirements

4.1 Introduction

The specifications of AMHS components in this Profile are based on the ISO/IEC ISPs and other specifications, which, in turn, are further refined by Annexes A to Q of this Profile. The following sections indicate which ISPs and which Annexes to this Profile shall be used in specifying each of the types of AMHS components identified in section 3 (UAs, MTAs, and MSs).

4.2 Conformance Requirements

An implementation claiming conformance to this specification shall meet the requirements of the Base Standards (ISO/IEC 10021), and the ISPs referenced in sections 4.3 to 4.7 applicable to the corresponding system type. The technical details are provided in Annexes A to P. Within each Annex, the notes in italics are advisory only and used to clarify the intent and development of each Annex.

An implementation claiming conformance to this specification shall additionally meet the requirements specified in sections 4.3 to 4.7 that apply to the particular type of system identified in section 4.3 including all those requirements contained in the referenced Annexes to this profile.

For each AMHS System Type identified in 4.3 below, Annex Q contains a corresponding Implementation Conformance Statement pro forma that is intended to document each implementation's conformance to the Base Standards, the referenced ISPs, Doc 9880, Part II [10] and the corresponding Annexes listed in sections 4.4 to 4.7. A claim of conformance for an implementation shall be supported by completion of the Profile Implementation Conformance Statement pro forma as described in Annex Q.

Support for the Extended ATS Message Handling Service is not mandated for conformance to this profile. However, an implementation for which conformance to this profile is claimed may additionally claim conformance to some or all of the requirements of the extended service. The requirements to be met for such additional conformance are specified by means of conditional 'c' requirements and notes at the bottom of tables in the following sections.

4.3 AMHS Systems and System Component Configurations

The following table specifies the different AMHS components required to construct an ATS Message User Agent System and an ATS Message Server to support the AFI AMHS Profile. Specifications of the corresponding systems components are given in sections 4.4 to 4.7.

Ref	System Component	ATS User System	ATS Message Server	Comments
1	IPM UA Content - See Annex A	m	-	For any UA exchanging ATS messages internationally
2	IPM UA – P3 Access - See section 4.4.1	c[1, 2]	-	"
3	IPM UA – P7 Access - See section 4.4.2	c[1, 2]	-	"
4	IPM UA – P7 (94) Access - See section 4.4.3	c[1, 2]	-	"
5	Co-located UA - See section 4.4.4	c[1, 3]	o[1, 3]	"
6	MTA - See section 4.5	-	m	For all MTAs supporting as International COM Centers
7	MS Support for P7 - See section 4.6	-	c[4]	
8	MS Support for P7 (94) - See section 4.7	-	c[5]	
9	Directory Information - See Annex K	o	o	Directory Information availability is indicated but not mandated.

Table 4.3.1: AMHS Systems and System Component Configurations

[1] if the Basic service or the AFI AMHS Profile is to be supported then at least one of the system components marked 1 is mandatory.

[2] if Extended service is to be supported at least one of those marked 2 is mandatory.

[3] Excluded (X) in the Extended Service if Secured Messages are to be generated.

[4] For any MS supporting P7 UAs exchanging ATS messages internationally m, else o.

[5] For any MS supporting P7 (94) UAs exchanging ATS Messages internationally m, else o.

4.4 IPM UA Requirements

There are three IPM User Agent scenarios which are illustrated in Figure 1:

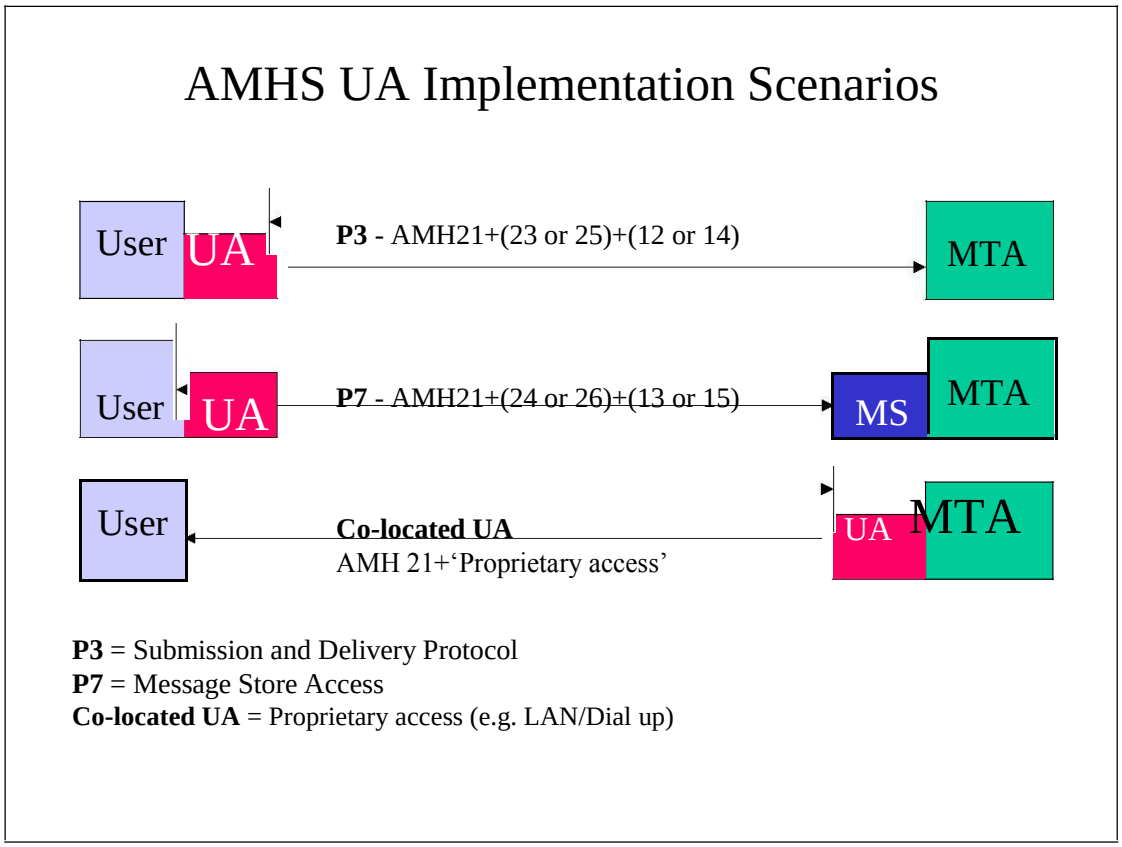

Figure 1: UA Implementation Scenarios

4.4.1 IPM UA using P3

This section applies where a AFI AMHS P3 based User Agent is to be procured.

A P3 User Agent for which conformance to this Profile is claimed shall conform to the following list of specifications:

Ref	Element	AFI AMHS Requirement	Specifications
1	IPM Content	m	Profile AMH21 – ISO/IEC ISP 12062-2 – IPM Content Annex A
2	IPM Use of P3	m[1]	Profile AMH23 & 25 – ISO/IEC ISP 12062-4 – IPM Requirements for MTS Access and MTS Access(94) – (P3)

Ref	Element	AFI AMHS Requirement	Specifications
			Annex C
3	P3	m[2]	Profile AMH12 & 14 – ISO/IEC ISP 10611-4 – Requirements for MTS Access and MTS Access(94) – (P3) Annex G
4	Upper Layers	m	Profile AMH1n – ISO/IEC ISP 10611-2 Common Messaging Specification of ROSE, RTSE, ACSE, Presentation and Session Protocols for use by MHS Annex J Annex N
5	Transport-RFC 1006/2126 – TCP	o[3]	Annex L
6	IP	o[3]	Annex M
7	IPSec	o[3]	Annex O
8	AMHS Cryptographic Profile	c[4]	Annex P
9	Directory Information	o	Annex K

Table 4.4.1: IPM UA using P3

[1] AMH23 is mandated for the Basic Service. Conformance to AMH25 may be additionally claimed for the Extended Service.

[2] AMH12 is mandated for the Basic Service. Conformance to AMH14 may be additionally claimed for the Extended Service.

[3] Locally specified by the ANSP. It must be either as stated in the requirement column, or must use ATN specification or specify another alternative.

[4] If extended Service then m else o.

4.4.2 IPM UA using P7

This section applies where a AFI AMHS P7 based User Agent is to be procured.

A P7 User Agent for which conformance to this Profile is claimed shall conform to the following list of specifications:

Ref	Element	AFI AMHS Requirement	Specifications
1	IPM Content	m	Profile AMH21 – ISO/IEC ISP 12062-2 – IPM Content Annex A
2	IPM Use of P7	m	Profile AMH24 – ISO/IEC ISP 12062-5 – IPM Requirements of Enhanced MS Access (P7) Annex D
3	P7	m	Profile AMH13 – ISO/IEC ISP 10611-5 – MS Access (P7) Annex H
4	Upper Layers	m	Profile AMH1n – ISO/IEC ISP 10611-2 Common Messaging Specification of ROSE, RTSE, ACSE, Presentation and Session Protocols for use by MHS Annex J Annex N
5	Transport-RFC 1006/2126 - TCP	o[1]	Annex L
6	IP	o[1]	Annex M
7	IPSec	o[1]	Annex O
8	AMHS Cryptographic Profile	c[2]	Annex P
9	Directory Information	o	Annex K

Table 4.4.2: IPM UA using P7

[1] Locally specified by the ANSP. It must be either as stated in the EUR AMHS Requirements column, or must use ATN specification or specify another alternative.

[2] If Extended Service then m else o.

4.4.3 IPM UA using P7 (94)

This section applies where a AFI AMHS P7 (94) based User Agent is to be procured.

A P7 (94) User Agent for which conformance to this Profile is claimed shall conform to the following list of specifications:

Ref	Element	AFI AMHS Requirement	Specifications
1	IPM Content	m	Profile AMH21 – ISO/IEC ISP 12062-2 – IPM Content Annex A
2	IPM Use of P7 (94)	m	Profile AMH26 – ISO/IEC ISP 12062-6 – IPM Requirements of Enhanced MS Access (94) (P7) Annex E
3	P7 (94)	m	Profile AMH15 – ISO/IEC ISP 10611-6 – MS Access-94 (P7) Annex I
4	Upper Layers	m	Profile AMH1n – ISO/IEC ISP 10611-2 Common Messaging Specification of ROSE, RTSE, ACSE, Presentation and Session Protocols for use by MHS Annex J Annex N
5	Transport-RFC 1006/2126 - TCP	o[1]	Annex L
6	IP	o[1]	Annex M
7	IPSec	o[1]	Annex O
8	AMHS Cryptographic Profile	c[2]	Annex P
9	Directory Information	o	Annex K

Table 4.4.3: IPM UA using P7 (94)

[1] Locally specified by the ANSP. It must be either as stated in column 1, or must use ATN specification or specify another alternative.

[2] If Extended Service then m else o.

4.4.4 IPM UA Co-located with MTA (with or without MS)

This section applies where a EUR AMHS Co-located based User Agent is to be procured.

An IPM User Agent integrated with MTA for which conformance to this Profile is claimed shall conform to the following list of specifications:

Ref	Element	EUR AMHS Requirement	Specifications
1	IPM Content	m	Profile AMH21 – ISO/IEC ISP 12062-2 – IPM Content Annex A
2	Underlying Proprietary Network and Protocols used to access the UA	–	Suppliers shall declare the name, version number etc. of the standards or products used

Table 4.4.4: IPM UA Co-located with MTA

4.5 MTA Requirements

This section applies where a AFI AMHS MTA is to be procured.

An MTA for which conformance to this Profile is claimed shall conform to the following list of specifications:

Ref	Element	AFI **AMHS Requirement**	Specifications
1	IPM Requirements of Message Transfer P1	m	Profile AMH22 – ISO/IEC ISP 12062-3 – IPM Requirements for Message Transfer – (P1) Annex B
2	Message Transfer Protocol – P1	m	ATS Messaging Addendum to Profile AMH11 – ISO/IEC ISP 10611-3 – MTS Transfer (P1) Annex F
3	IPM Requirements of Message Submission and Delivery Service P3	c[1]	Profile AMH23 & 25 – ISO/IEC ISP 12062-4 – IPM Requirements for MTS Access and MTS Access(94) – P3 Annex C

Ref	Element	AFI **AMHS Requirement**	Specifications
4	Message Submission and Delivery Service P3	c[1]	Profile AMH12 & 14 – ISO/IEC ISP 10611-4 – Requirements for MTS Access and MTS Access(94) – (P3) Annex G
5	Upper Layers	m	Profile AMH1n – ISO/IEC ISP 10611-2 Common Messaging Specification of ROSE, RTSE, ACSE, Presentation and Session Protocols for use by MHS Annex J Annex N
6	Transport-RFC 1006/2126 - TCP	m	Annex L
7	IP	m	Annex M
8	IPSec	o	Annex O
9	Directory Information	o	Annex K

Table 4.5.1: MTA Requirements

[1] If MTA supports P3 UAs or MSs then m, else o.

4.6 MS Requirements

This section applies where a AFI AMHS P7 based Message Store is to be procured.

A Message Store for which conformance to this Profile is claimed shall conform to the following list of specifications:

Ref	Element	AFI **AMHS Requirement**	Specifications
1	IPM Content	m	Profile AMH21 – ISO/IEC ISP 12062-2 – IPM Content Annex A
2	IPM Use of P7	m	Profile AMH24 – ISO/IEC ISP 12062-5 – IPM Requirements of Enhanced MS Access (P7)

Ref	Element	AFI **AMHS Requirement**	Specifications
			Annex D
3	P7	m	Profile AMH13 – ISO/IEC ISP 10611-5 – MS Access (P7) Annex H
4	Upper Layers	m	Profile AMH1n – ISO/IEC ISP 10611-2 Common Messaging Specification of ROSE, RTSE, ACSE, Presentation and Session Protocols for use by MHS Annex J Annex N
5	Transport-RFC 1006/2126 - TCP	o[1]	Annex L
6	IP	o[1]	Annex M
7	IPSec	o[1]	Annex O
3	AMHS Cryptographic Profile	c[2]	Annex P

Table 4.6.1: MS Requirements

[1] Locally specified by the ANSP. It must be either as stated in the requirements column, or must use ATN specification or specify another alternative

[2] If Extended Service then m else o.

4.7 MS (94) Requirements

This section applies where a AFI AMHS Message Store (94) is to be procured.

A P7 (94) Message Store for which conformance to this Profile is claimed shall conform to the following list of specifications:

Ref	Element	AFI **AMHS Requirement**	Specifications
1	IPM Content	m	ATS Messaging Addendum to Profile AMH21 – ISO/IEC ISP 12062-2 – IPM Content

Ref	**Element**	AFI **AMHS Requirement**	**Specifications**
			Annex A
2	IPM Use of P7 (94)	m	Profile AMH26 – ISO/IEC ISP 12062-6 – IPM Requirements of Enhanced MS Access (94) (P7) Annex E
3	P7 (94)	m	Profile AMH15 – ISO/IEC ISP 10611-6 – MS Access-94 (P7) Annex I
4	Upper Layers	m	Profile AMH1n – ISO/IEC ISP 10611-2 Common Messaging Specification of ROSE, RTSE, ACSE, Presentation and Session Protocols for use by MHS Annex J – ISP Addendum Annex N – Upper Layer Addressing
5	Transport-RFC 1006/2126 - TCP	o[1]	Annex L
6	IP	o[1]	Annex M
7	IPSec	o[1]	Annex O
3	AMHS Cryptographic Profile	c[2]	Annex P

Table 4.7.1: MS (94) Requirements

[1] Locally specified by the ANSP. It must be either as stated in the requirements column, or must use ATN specification or specify another alternative.

[2] If Extended Service then m else o.

A. ANNEX A (NORMATIVE) – IPM CONTENT

AMHS Addendum to Profile AMH21 – ISO/IEC ISP 12062-2 IPM Content

A.1 Introduction

This is an addendum to ISO/IEC ISP 12062-Part 2 – AMH21 - IPM Content (the ISP), and should be used in conjunction with that ISP. It contains additional requirements to those specified in the ISP for ATS Message User Agents.

Note. – Summary:

The IPM content has a high significance for end-to end ATS messaging;

The ISP (12062-2) mandates most of the required heading, OR-Naming, content types and Body Parts used for ATS messaging. However it is necessary to ensure that Business Class messaging, general-text, Ia5 text and File Transfer body parts may also be correctly mandated together with the required optional functional group for DL in the appropriate profiles;

Additional UA requirements concerning ATS Message Header Generation, potentially Message Legal Recording, use of message priorities, interpretation of UTC Time, and use of DL Expansion prohibition are also specified;

Note that the IPM Profile itself makes no mention of the S0 Security functional group since it is purely a message 'envelope' based technique which is more related to the P1/P3/P7 profiles and which are specified to include S0 in other Annexes.

A.2 AFI AMHS Requirement

A.2.1 ISP Conformance

An AMHS User Agent shall conform to Profile AMH21 – ISO/IEC ISP 12062-2 – IPM Content.

A.2.2 Additional Requirements to the ISP

The following tables (A.0.6, A.1.3, A.1.3.1 and A.1.3.3) have been adapted from, and refer to the tables of the same title as those in ISO/IEC ISP 12062-2. They specify additional mandatory requirements that express restrictions on a set of rows of the AMH21 profile that are referred to using their references used in ISO/IEC ISP 12062-2. Implementations for which conformance to this Profile is claimed shall implement the additional mandatory elements.

----------Begin of references to ISO/IEC ISP 12062-2----------

A.0.6 Statement of profile conformance

Ref	Question	ISP	Doc 9880		AFI AMHS	Comments
			Basic Service	**Ext.** Service		
2	Are all mandatory requirements of any of the following optional functional groups implemented?					
2.2	IPM Security (SEC)	o	o	m	o	class(es): S0 – Common Messaging
2.5	IPM Business Class (BC)	o	o	m	o	See Doc 9880, Part II - 3.1.4.2.1

A.1.3 IPM body

Ref	Element	ISP	Doc 9880		AFI AMHS	Notes/ References
		Origin/Rec	**Basic** Service **origin /rec**	**Extended** Service **origin /rec**	**origin/rec**	
1	ia5-text	o/m	o/m	o/m	o/m	
1.2	data	m/m	m/m	m/m	m/m	See Doc 9880, Part II - 3.3.3
12	extended	m/m	m/m	m/m	m/m	

A.1.3.1 Extended body part support

Ref	Extended Body Part Type	ISP Origin/ Rec.	Doc 9880		AFI AMHS	Notes/ References
			Basic Service	**Extended** Service		
			Orig/Rec	**Orig/Rec**	**Orig/rec**	
1	ia5-text-body-part	o/m	o/m	o/m	o/m	see A.1.3/1
11	general-text-body-part	m/m	m/m	m/m	m/m	see Doc 9880, Part II - 3.3.3 and Table 3-1 Part 4
12	File-transfer-body-part	o/m	o/m	m/m	m/m	See Doc 9880, Part II - Table 3-2

A.1.3.3 General text repertoire support

Ref	Repertoire set description	Repertoire identifiers	ISP				Doc 9880 Basic & Extended Service		EUR AMHS Requirement	
			Origi-nation		Recep-tion		Origin/Rec		Origin/ Rec	
			A	B	A	B	A	B	A	B
1	Basic (ISO 646)	{1,6}	m	m	m	m	m/m	m/m	m	m
2	Basic-1 (ISO 8859-1)	{1,6,100}	o	m	o	m	-	o/o	o/o	o/o

A.1.5 Common data types

Ref	Element	ISP	Doc 9880		AFI AMHS	Notes and References
		Origin/ Rec	Basic Service	Extended Service		
			Origin/ Rec	Origin/ Rec	Origin/Rec	
1	RecipientSpecifier					
1.2	notification-requests	o/m	m/m	m/m	m/m	see Doc 9880, Part II - 3.3.6
1.2.1	rn	o/o	m/m	m/m	m/m	see Doc 9880, Part II - 3.3.6
1.2.2	nrn	o/m	m/m	m/m	m/m	
2	ORDescriptor					
2.1	formal-name	m^1/m^1	m^1/m^1	m^1/m^1	m^1/m^1	see A.1.7 in ISO/IEC ISP10611-3 see also Doc 9880, Part II - 3.3.2.1

m^1 - the requirements for support of OR-names are specified in clause 8 of ISO/IEC ISP 12062-1 (i.e. a claim of support of the formal-name element means that at least the minimum requirements of ISO/IEC ISP 12062-1 with respect to the component elements of OR-names are met).

----------End of references to ISO/IEC ISP 12062-2----------

A.2.3 Additional Implementation Capabilities for the AFI AMHS Profile (from Doc 9880, Part II [10])

A.2.3.1 Generation of AMHS Messages

ATS Message User Agents shall be capable of constructing and receiving ATS Messages in an IPM Ia5 body part as specified in Doc 9880, Part II [10], section 3.3.

Note. – Generation of ATS Messages may differ for certain cases where the UA conforms to the Extended Service.

A.2.3.2 Generation of ATS 'SS' priority messages

User Agents used to create ATS messages shall automatically select the DL-Expansion-Prohibition service when creating ATS messages with an 'SS' priority indicator.

A.2.3.3 Use of DL expansion prohibition

ATS Message User Agents shall prevent users from selecting the DL-Expansion-Prohibition service for all ATS messages with the exception of ATS messages with an 'SS' priority indicator.

A.2.3.4 Use of the 'urgent' MTS message priority

ATS Message User Agents shall prevent users from selecting the MHS message priority 'urgent' for any messages with the exception of messages with an 'SS' ATS-message-priority indicator. ATS Message User Agents shall also automatically assign the priority 'urgent' to each message carrying an 'SS' ATS-message-priority indicator.

A.2.3.5 ATS Message Legal Recording

ATS Message User Agents may optionally be required to perform Legal Recording of message traffic as specified in the Doc 9880, Part II [10], sections 3.1.3 and 2.7.

A.2.3.6 Interpretation of UTC Time

An ATS Message User Agent shall interpret the value of UTC time as specified in the Doc 9880, Part II [10], section 3.1.2.4.

A.2.3.7 Requests for Receipt Notifications

ATS Message User Agents shall only allow requests for Receipt Notification Requests if the ATS Message has an 'SS' Priority.

A.2.3.8 Message Size Supported

The maximum message length that ATS Message User Agents are capable of generating and receiving shall be a configuration parameter that can be adjusted as operational requirements evolve in the future. It is strongly recommended that each UA should have a static capability of generating and receiving messages of at least 64 Kbytes length.

Note that the deliverable maximum content length that an MTA may deliver at any given time may be controlled by use of the P3 Delivery Control operation (permissible-maximum-content-length) and the P3 Register operation (permissible- maximum- content-length). However, ANSPs will have to specify this capability for their UAs and MTAs as a local matter.

A.2.4 Additional Extended Service-specific Implementation Capabilities

A.2.4.1 Use of the Business Class Heading Fields

The ATS Messaging User Agent supporting the Extended Service shall be capable of setting the Business Class Heading fields values as specified in Doc 9880, Part II [10], section 3.3.4 if, and only if it can be determined that the originator and all of the intended recipients systems support the Extended Service (i.e. they all support the IPM Heading Extension

Use of the Business Class Heading Fields remains optional in the AFI AMHS Profile.

A.2.4.2 Use of parameters in the file-transfer body part

When forwarding binary data with file-transfer body parts for the included file transfer parameters "default values" shall apply as indicated in the table below. Other or additional parameter types and/or values may be used by multilateral agreement.

----------Begin of references to ISO/IEC ISP 12062-2----------

A.1.3.3 File transfer parameters

Ref	**Extended Body Part Type**	**Origination**		**Reception**		**EUR AMHS** Orig / Rec	**Comment**
		Base	**Profile**	**Base**	**Profile**		
1	related-stored-file	o	o	o	o	-	
2	contents-type	o	m	o	m		
2.1	document-type	o	o	o	o		
2.1.1	document-type-name	m	m	m	m	m/m	See A.2.4.2.1
3	environment	o	m	o	m		
3.1	application-reference	o	m	o	m		
3.1.1	registered-identifier	o	m	o	m	o/m	See A.2.4.2.2
3.4	user-visible-string	o	m	o	m	o/m	See A.2.4.2.6
4	compression	o	o	o	o	-	
5	file-attributes	o	m	o	m		
5.1	pathname	o	m	o	m		
5.1.1	incomplete-pathname	o	m	o	m	o/m	See A.2.4.2.3
5.5	date-and-time-of-last-modification	o	m	o	m	o/m	See A.2.4.2.4
5.13	object-size	o	m	o	m		
5.13.2	actual-values	o	m	o	m	o/m	See A.2.4.2.5
6	extensions	o	o	o	o	-	

----------End of references to ISO/IEC ISP 12062-2----------

A.2.4.2.1 The element *document-type-name* in the *document-type* element of the *contents-type* parameter shall take its default value in conformance with ISO/IEC 10021-7:2003 clause 7.4.12, which is the OID value {iso(1) standard(0) 8571(8571) document-type(5) unstructured-binary(3)}.

A.2.4.2.2 The element *registered-identifier* in the *application-reference* element of the *environment* parameter shall:

a. be optionally generated by the originator; and

b. when present, take either by default the OID value registered by the Electronic Messaging Association (EMA) to represent the abstract-value "unknown-attachment", which is the OID value {2.16.840.1.113694.2.2.1.1} or one of the registered OID values listed in A.2.4.2.6.

A.2.4.2.3 The element *pathname* in the *file-attributes* parameter shall:

a. be optionally generated by the originator using the *incomplete-pathname* element; and

b. when present, contain a file-name value, without preceding path information to be potentially used for local storage of the included data.

A.2.4.2.4 The element *date-and-time-of- last-modification* in the *file attributes* parameter shall be optionally generated by the originator.

A.2.4.2.5 The element *actual-values* of the *object-size* element in the *file-attributes* parameters shall:

a. be optionally generated by the originator; and

b. when present, take the value representing the size of the included data in bytes.

A.2.4.2.6 The element *user-visible-string* of the environment parameter shall be present in cases where the element *registered -identifier* is present and set to an OID value other than the default one (see A.2.4.2.2 b). In these cases, the OID value of the element *registered-identifier* and the corresponding value of the element *user-visible-string* shall be assigned according to the following Table of registered sets of values:

OID Value (*registered-identifier*)	**Application Program (*user-visible-string*)**	**Organisation/ Authority**
1.3.27.8.1.0 {icao-atn-amhs application(1) digital-notam(0)}	Digital NOTAM	AFSG
1.3.27.8.1.1 {icao-atn-amhs application(1) digital-fpl(1)}	Digital FPL	AFSG
1.3.27.8.1.2 {icao-atn-amhs application(1) digital-met(2)}	Digital MET	AFSG

OID Value (*registered-identifier*)	**Application Program (*user-visible-string*)**	**Organisation/ Authority**
1.3.27.8.1.3 {icao-atn-amhs application(1) bufr(3)}	BUFR	AFSG
1.3.27.8.1.4 {icao-atn-amhs application(1) grib2(4)}	GRIB Edition 2	AFSG

Table A.2.4.2: registered OID values

A.2.4.2.7 Further OID values and application programs may be allocated on request using the Change Control Procedure of the AFI AMHS Manual (see Attachment A of the AFI AMHS Manual).

B. ANNEX B (NORMATIVE) – IPM REQUIREMENTS OF P1

AMHS Addendum to Profile AMH22 – ISO/IEC ISP 12062- 3 – IPM Requirements for Message Transfer – (P1)

B.1 Introduction

This is an addendum to ISO/IEC ISP 12062-Part 3 – AMH22 - IPM Requirements for Message Transfer (P1) and should be used in conjunction with the ISP. It contains additional requirements to those specified in the ISP for AMHS MTAs used to transfer ATS Messages to each other.

Note. – Summary:

P1 is largely transparent to IPM, so IPM places minimal requirements on it;

However, it is necessary to ensure that the FG for DL is selected to ensure transparency, and that MTAs can expand DLs.

The P1 profile itself contains a number of requirements that stem directly from ATS messaging that are not directly related to IPM.

B.2 AFI AMHS Requirement

B.2.1 ISP Conformance

An AMHS MTA shall conform to Profile AMH22 – ISO/IEC ISP 12062-3 – IPM Requirements of P1.

B.2.2 Additional Requirements to ISP

The following table (A.0.6 – a table of ISO/IEC ISP 12062- 3) specifies additional requirements that express restrictions on a set of rows of the AMH22 profile that are referred to using their references in ISO/IEC ISP 12062-3.

----------Begin of references to ISO/IEC ISP 12062-3----------

A.0.6 Statement of profile conformance

Ref	Question	ISP	Doc 9880		EUR AMHS	Comments
			Bas	Ext		
4	Are all mandatory requirements of any of the following optional functional groups implemented?					
4.2	IPM Distribution List (DL)	o	m	m	m	
4.7	IPM Security (SEC)	o	o	m	o	class(es): S0 – Common Messaging

End of references to ISO/IEC ISP 12062-3----------

C. ANNEX C (NORMATIVE) – IPM REQUIREMENTS OF P3

AMHS Addendum to Profile AMH23 & 25 – ISO/IEC ISP 12062-4 – IPM Requirements for MTS Access and MTS Access(94) – (P3)

C.1 Introduction

This is an addendum to ISO/IEC ISP 12062-Part 4 – AMH23 and 25 - IPM Requirements for MTS Access and MTS Access(94) (P3), and should be used in conjunction with that ISP. It contains additional requirements to those specified in the ISP for AMHS MTS Users (UAs and MSs) and MTAs used for submission and delivery of ATS messages.

Note. – Summary:

P3 is largely transparent to IPM, so IPM places minimal requirements on

it; However, it is necessary to ensure that the FG for DL is selected;.

The P3 profile itself contains a number of further requirements that stem directly from ATS messaging that are not directly related to IPM, and includes requirements for the dynamic generation of Message Tokens for submission of Secure ATS messages for the Extended AMHS service. Message Tokens are not required for the AFI AMHS Profile.

C.2 AFI AMHS Requirement

C.2.1 ISP Conformance

The AMHS UA or MTA implementation shall conform to Profile AMH23 and AMH25 – ISO/IEC ISP 12062-4 – IPM Requirements of MTS Access and MTS Access (94). Conformance to the AMH25 profile is not mandated for the Basic AMHS Service.

C2.2 Additional Requirements to ISP

The following table (A.0.7 – a table of ISO/IEC ISP 12062-4) specifies additional requirements that express restrictions on a set of rows of the AMH23 and AMH25 profiles that are referred to using their references in ISO/IEC ISP 12062-4.

----------Begin of references to ISO/IEC ISP 12062-4----------

A.0.7 Statement of profile conformance

Ref	Question	ISP	Doc 9880		EUR AMHS	Comments
			Bas	Ext		
3	Are all mandatory requirements of any of the following optional functional groups implemented?					
3.2	IPM Distribution List (DL)	o	m	m	m	

Ref	Question	ISP	Doc 9880		EUR AMHS	Comments
			Bas	Ext		
3.7	IPM Security (SEC)	o	o	m	o	class(es): S0 – Common Messaging

End of references to ISO/IEC ISP 12062-4----------

D. ANNEX D (NORMATIVE) – IPM REQUIREMENTS OF P7

AMHS Addendum to Profile AMH24 – ISO/IEC ISP 12062-5 – IPM Requirements of Enhanced MS Access (P7)

D.1 Introduction

This is an addendum to ISO/IEC ISP 12062-Part 5 – AMH24 - IPM Requirements of Enhanced MS Access (P7) (the ISP), and should be used in conjunction with the ISP. It contains additional requirements to those specified in the ISP for AMHS User Agents used to retrieve messages from a Message Store using the Enhanced MS Access (P7) protocol.

Note. – Summary:

P7 must implement an appropriate set of MS IPM attributes to support ATS messaging. Most are mandated by the ISPs;

It is necessary to ensure that the FG for DL is selected, and that the MS and MS user can deal with the appropriate Heading Attributes and ATS body part types.

Selection of the IPM BC Functional group automatically selects the appropriate heading field attributes for BC (as used in ATS messaging);

It is necessary to specify the required body part types used to support ATS messaging;

Support for IPM Content Types is mandated in the ISPs;

The P7 profile itself contains a number of further requirements that stem directly from ATS messaging that are not directly related to IPM, and includes requirements for the dynamic generation of Message Tokens for Secure ATS messages and support of the S0 security functional group. S0 is not mandated by the EUR AMHS Profile.

D.2 AFI AMHS Requirement

D.2.1 ISP Conformance

An AMHS UA or MS shall conform to Profile AMH24 – ISO/IEC ISP 12062-5 – IPM Requirements of Enhanced MS Access.

D.2.2 Additional Requirements to ISP

The following tables (A.0.7 and A.1.12.1 of ISO/IEC ISP 12062-5) specify additional requirements that express restrictions on a set of rows of the AMH24 profile that are referred to using their references in ISO/IEC ISP 12062-5.

----------Begin of references to ISO/IEC ISP 12062-5----------

A.0.7 Statement of profile conformance

Ref	Question	ISP	Doc 9880		EUR AMHS	Comments
			Bas	Ext		
3	Are all mandatory requirements of any of the following optional functional groups implemented?					
3.2	IPM Distribution List (DL)	o	m	m	m	
3.7	IPM Security (SEC)	o	o	m	o	class(es): S0 Common Messaging
3.9	IPM Business Class (BC)	o	o	m	o	

A.1.12.1 Extended body part attribute support

Ref	Extended Body Part Attribute	UA		MS		UA EUR AMHS	MS EUR AMHS	Notes/References
		ISP	Doc 9880 Bas/Ext	ISP	Doc 9880 Bas/Ext			
1	ia5-text-body-parts	o	o/o	m	m/m	m	m	
11	general-text-body-parts	o	m/m	m	m/m	m	m	
12	file-transfer-body-part	o	o/m	o	o/m	m	m	See Doc 9880, Part II – Table 3-2

End of references to ISO/IEC ISP 12062-5----------

E. ANNEX E (NORMATIVE) – IPM REQUIREMENTS OF P7 (94)

ATS Messaging Addendum to Profile AMH26 – ISO/IEC ISP 12062-6 – IPM Requirements of Enhanced MS Access (94) (P7)

E.1 Introduction

This is an addendum to ISO/IEC ISP 12062-Part 6 – AMH26 - IPM Requirements of Enhanced MS Access (94) (P7) (the ISP), and should be used in conjunction with that ISP. It contains additional requirements to those specified in the ISP for AMHS User Agents used to retrieve messages from a Message Store using the Enhanced MS Access (94) (P7) protocol.

Note. – Summary:

P7 must implement an appropriate set of MS IPM attributes to support ATS messaging. Most are mandated by the ISPs;

It is necessary to ensure that the FG for DL is selected, and that the MS and MS user can deal with the appropriate Heading Attributes and ATS body part types.

Selection of the Business Class Messaging Functional Group automatically selects the appropriate heading field attributes for Business Class (as used in ATS messaging);

It is necessary to specify the required body part types used to support ATS messaging;

Support for IPM Content Types is mandated in the ISPs;

The P7 profile itself contains a number of further requirements that stem directly from ATS messaging that are not directly related to IPM, and includes requirements for the dynamic generation of Message Tokens for Secure ATS messages and support of the S0 security functional group. S0 is not mandated by the EUR AMHS Profile.

E.2 AFI AMHS Requirement

E.2.1 ISP Conformance

An AMHS UA and MS (94) shall conform to Profile AMH26 – ISO/IEC ISP 12062-6 – IPM Requirements of Enhanced MS Access (94) (P7).

E.2.2 Additional Requirements to ISP

The following tables (A.0.7, A.1.15.1 and A.1.15.3 of ISO/IEC ISP 12062 -6) specify additional requirements that express restrictions on a set of rows of the AMH26 profile that are referred to using their references in ISO/IEC ISP 12062-6.

----------Begin of references to ISO/IEC ISP 12062-6----------

A.0.7 Statement of profile conformance

Ref	Question	ISP	Doc 9880		AFI AMHS	Comments
			Bas	Ext		
3	Are all mandatory requirements of any of the following optional functional groups implemented?					
3.2	IPM Distribution List (DL)	o	m	m	m	
3.7	IPM Security (SEC)	o	o	m	o	class(es): S0 Common Messaging
3.31	IPM Business Class (BC)	o	o	m	o	

A.1.15.1 Support of IPM-specific attributes in the Stored-message subordinate entry-classes

Ref	Attribute	UA	MS	AFI AMHS		Notes/References
		ISP	ISP	UA	MS	
50	ia5-text-body-parts	o	m	m	m	
51	ia5-text-data	o	o	m	m	
52	ia5-text-parameters	o	o	m	m	

A.1.15.3 Extended body part attribute support in Stored-message subordinate entry-classes

Ref	Attribute	UA	MS	AFI AMHS		Notes/References
		ISP	ISP	UA	MS	
1	ia5-text-body-part	o	m	m	m	
11	general-text-body-part	m	m	m	m	
12	file-transfer-body-part	m	m	m	m	See Doc 9880, Part II – Table 3-2

End of references to ISO/IEC ISP 12062-6----------

F. ANNEX F (NORMATIVE) – REQUIREMENTS OF MESSAGE TRANSFER PROTOCOL - P1

AMHS Addendum to Profile AMH11 – ISO/IEC ISP 10611-3 – MTS Transfer (P1)

F.1 Introduction

This is an addendum to ISO/IEC ISP 10611- Part 3 – AMH11 – MTS Transfer (P1), and should be used in conjunction with the ISP. It contains additional requirements to those specified in the ISP for ATS Message Servers used to transfer ATS Messages.

Note. – Summary:

Since the ISPICs requires full transparency for message transfer for all possible envelope and content fields, there are no extra requirements for tables A1 and A2 of the PICS that affect the P1 Protocol static requirements. However:

Table A.0.6 has been used to select the required Optional Functional Groups for DL and S0;

Table A3 has been extended to incorporate a number of ATS specific implementation requirements with respect to MTA routing evaluation of the XF and CAAS addressing attributes;

Table A.3.4 and A.3.5 have been extended to accommodate ATS specific implementation requirements of Message Server MTA components.

F.2 AFI AMHS Requirements

F.2.1 ISP Conformance

An AMHS MTA shall conform to Profile AMH11 – ISO/IEC ISP 10611-3 – MTS Transfer.

F.2.2 Additional Requirements to ISP

The following tables (A.0.6and A.3.1 of ISO/IEC ISP 10611 -3) specify additional requirements that express restrictions on a set of rows of the AMH11 profile that are referred to using their references in AMH11 – ISO/IEC ISP 10611-3).

----------Begin of references to ISO/IEC ISP 10611-3----------

A.0.6 Statement of profile conformance

Ref	Question	ISPs	Doc 9880 Bas/Ext	AFI AMHS	Comments
3	Are all mandatory requirements of any of the following optional functional groups implemented?				
3.2	Distribution List (DL)	o	m/m	m	class(es):

Ref	Question	ISPs	Doc 9880 Bas/Ext	AFI AMHS	Comments
3.7	Security (SEC)	o	o/m	o	class(es): S0 – Common Messaging

A.3.1 Routing capability

The following additions to table A.3.1 ensure that conformant MTAs will be able to route messages on all of the XF and CAAS address-form attributes.

Ref	OR-Address Attribute	ISP	AFI AMHS	Comments
1	country-name[1]	o	m	
2	administration-domain-name[2]	o	m	
6	private-domain-name	o	m	
7	organization-name	o	m	
	teletex-organization-name [3] universal-organization-name[3]	o	o	
10	organizational-unit-names	o	m	
	teletex-organizational-unit-names[3] universal-organizational-unit-names[3]	o	o	
11	common-name	o	m	
	teletex-common-name[3] universal-common-name[3]	o	o	

[1] In particular, it shall be ensured that messages can be routed using the country name value = 'XX'.

[2] In particular, it shall be ensured that messages can be routed using the Administration Domain Name = 'ICAO'.

[3] Not required for support of the CAAS addressing scheme.

----------End of references to ISO/IEC ISP 10611-3----------

F.2.3 Implementation capabilities

The following requirements are in addition to those specified in ISO/IEC ISP 10611-3).

F.2.3.1 ATS Message Legal Recording

MTAs shall be capable of generating and holding long term message traffic logs for 'legal recording' as specified in the Doc 9880, Part II [10], sections 3.2.3 and 2.7. These requirements are mandatory for conformance to theAFI AMHS Profile.

F.2.3.2 Interpretation of UTC Time

An MTA shall interpret the value of UTC time as specified in Doc 9880, Part II [10], 3.1.2.4. These requirements are mandatory for conformance to the AFI AMHS Profile.

F.2.4 Implementation constraints

The following requirements are in addition to those specified in ISO/ISP 10611-3.

F.2.4.1 Number of Simultaneous P1 Associations

Suppliers shall declare the maximum number of simultaneous P1 Associations that can be maintained by the MTA with other MTAs.

Note. – Within AFI, each international MTA should be able to interconnect on a potentially simultaneous basis to each of the international MTAs of all other countries within EUR using P1 (i.e. in the region of 40 other MTAs). In addition, each international MTA should be capable of maintaining at least two simultaneous P1 associations to each MTA supporting users within that country (the number depends upon the topology and connectivity of MTAs within that country). Additionally, any MTA that acts as an inter -Regional Entry/Exit point should be capable of supporting two simultaneous associations to the corresponding MTA of the other Region.

F.2.4.2 MTA Message Transit Time

Suppliers shall state the maximum transit time per message due to the MTA (from last byte received by the MTA to the last byte being transmitted).

The SPACE Final Report requires a maximum transit time within Europe of 10 seconds to meet the high quality of service. Since a message transiting Europe will need to transit several MTAs and P1 protocol instances connecting them, each MTA will need to process each message in a fraction of the 10 seconds overall target. This fraction will depend solely on the configuration of the ANSP's internal topology and routing strategy. In general, the overall transit time allocated to each ANSP will be 3.3 seconds.

F.2.4.3 Minimum message size support

The SPACE Final Report requires that MTAs shall be capable of taking submission, transferring and delivering messages of at least 2 Mbytes overall length.

G. ANNEX G (NORMATIVE) – REQUIREMENTS OF MESSAGE SUBMISSION AND DELIVERY PROTOCOL – P3 AMHS Addendum to Profiles AMH12 & 14 – ISO/IEC ISP 10611-4 – Requirements for MTS Access and MTS Access(94) – (P3)

G.1 Introduction

This is an addendum to ISO/IEC ISP 10611-Part 4 – AMH12 and 14 - Requirements for MTS Access and MTS Access(94) (P3) and should be used in conjunction with the ISP. It contains additional requirements to those specified in the ISP for AMHS MTS Users (UAs and MSs) and MTAs used for submission and delivery of ATS messages.

Note. – Summary:

There are two parts to P3, an MTA part and an MTS user part;

The MTA part is required to be transparent (as is the MTS as a whole). The MTS user part is also required to be 'transparent', but the MTS User part is required to generate certain ATS message specific components such as the Message Token, CAAS + XF Address Attributes, and certain body part types;

Also, many of the specifications (i.e. the operations apart from Submission and Delivery) are purely local, and are not profiled here. Individual ANSPs may have their own preferences (e.g. for BIND credentials and Administration) here;

So, the basic requirements of the ISPs satisfy most of the requirements. However, the P3 profile is enhanced by this addendum in tables A.0.7, A.3.1, A.3.2, A.3.4 and A.3.5 to ensure that the MTS User component and the MTA can transfer, deliver, generate and receive several items that are required by for ATS messaging, namely: the Message Token, ia5, general text and File Transfer body parts, IPM(88), DL and S0 functional groups, OR-Address attributes.

G.2 AFI AMHS Requirements

G.2.1 ISP Conformance

An AMHS UA or MS shall conform to Profile AMH12 as specified in ISO/IEC ISP 10611-4 – MTS Access and MTS Access 94.

An AMHS UA or MS may additionally conform to Profile AMH14 as specified in ISO/IEC ISP 10611-4 – MTS Access and MTS Access 94.

G.2.2 Additional Requirements to ISP

The following tables (A.0.7, A.1.9, A.3.1, A.3.2 and A.3.4 of ISO/IEC ISP 10611 - 4) specify additional ATS messaging requirements of the P3 implementation that express restrictions on a set of rows of the AMH12 & AMH14 profiles that are referred to using their references in ISO/IEC ISP 10611 - 4.

----------Begin of references to ISO/IEC ISP 10611-4----------

A.0.7 Statement of profile conformance

Ref	Question	ISP	Doc 9880 Bas/Ext	AFI AMHS	Comments
2	Are all mandatory requirements of any of the following optional functional groups implemented?				
2.2	Distribution List (DL)	o	m/m	m	only applicable in the case of an MTA class(es):
2.7	Security (SEC)	o	o/m	o	class(es): S0 – Common Messaging

A.2.7 Security (SEC) (Optional Functional Group)

A.2.7.8 Extension data types

Selection of the S0 Functional Group mandates the ability of MTAs and the MTS user to be able to deal with the Message Token, however, the dynamic capability for the MTS user is mandated in section G.4.1 of this profile.

A.3.1 Content types supported

Ref	Content Type	ISP	Doc 9880 Bas/Ext	AFI AMHS	Comments
1.2	interpersonal-messaging-1984 (2)	o	-	-	not used
1.3	interpersonal-messaging-1988 (22)	o	m/m	m	

A.3.2 Encoded information types supported

Ref	Encoded Information Type	ISP	Doc 9880		AFI AMHS	Comments
			Submit	Delivery		
		Submit Deliv	Bas/Ext	Bas/Ext	Subm/Del	
1.2	ia5-text (2)	o/m	m/m	m/m	m/m	
2	extended					
2.1						In support for general-text body part as in ISO/IEC 10021-7 B.2
2.1.1	OID {iso(1) standard(0) motis(10021) ipms(7) cs(1) eit-authority(0) 1}	m/m	m/m	m/m	m/m	m in support for of Basic (ISO 646) repertoire o in support for Basic-1(ISO 8859-1) repertoire

Ref	Encoded Information Type	ISP Submit Deliv	Doc 9880 Submit Bas/Ext	 Delivery Bas/Ext	AFI AMHS Subm/Del	Comments
2.1.2	OID {iso(1) standard(0) motis(10021) ipms(7) cs(1) eit-authority(0) 6}	m/m	m/m	m/m	m/m	m in support for of Basic (ISO 646) repertoire o in support for Basic-1(ISO 8859-1) repertoire
2.1.3	OID {iso(1) standard(0) motis(10021) ipms(7) cs(1) eit-authority(0) 100}	o/o	o/o	o/o	o/o	o in support for Basic-1(ISO 8859-1) repertoire
2.1.4	OID {joint-iso-itu-i(2) mhs(6) ipms(1) eit(12) file-transfer(0)	o/o	o/o	m/m	m/m	m in support for the File Transfer Body Part

A.3.4 Delivery capability

Ref	OR-Address Attribute	ISP	Doc 9880 Bas/Ext	AFI AMHS	Comments
1	country-name	0	m/m	m	
2	administration-domain-name	o	m/m	m	
6	private-domain-name	o	m/m	m	
7	organization-name	o	m/m	m	
	teletex-organization-name[1] universal-organization-name[1]	o	o	o	
10	organizational-unit-names	o	m/m	m	
	teletex-organizational-unit-names[1] universal-organizational-unit-names[1]	o	o	o	
11	common-name	o	m/m	m	
	teletex-common-name[1] universal-common-name[1]	o	o	o	

[1] – Not required to support the CAAS and XF addressing schemes.

A.3.5 Implementation constraints

A.3.5.1 Maximum P3 Associations for MTA

The supplier shall state the maximum number of MTS-Access or MTS Access (94) Associations that can be simultaneously supported by an MTA.

----------End of references to ISO/IEC ISP 10611-4----------

G.3 Additional requirements to support AMHS

G.3.1 Additional MTS User requirement for Generation Secure Messages for the Extended ATS Message Handling Service

AMH12 and AMH14 specify the static requirements for the Message Token in Table A.1.9/4. The following table specifies the corresponding requirement for dynamic generation of Message Token Fields for MTS Users conforming to the S0 Functional Group when generating a secure ATS message. Refer also to the Doc 9880, Part II [10] - Table3-3. Use of Security Elements (Message Token) in the Extended ATS Message Handling Service.

Begin of references to ISO/IEC ISP 10611-4----------

A.1.9 Extension Data Types:

Ref	Element	MTS-User Static Requirement			Dynamic action for secure message	Notes/References
		ISP	Doc 9880 Bas/Ext	AFI AMHS		
4	MessageToken	o	o/m	o	G	
4.1	token-type-identifier	m	m	o	G	See Doc 9880, Part II - 3.1.4.3.6
4.2	asymmetric-token	m	m	o	G	See Doc 9880, Part II - 3.1.4.3.7
4.2.1	signature-algorithm-identifier	m	m	o	G	See Doc 9880, Part II - 3.1.4.3.8
4.2.2	name	m	m	o	G	See Doc 9880, Part II - 3.1.4.3.9
4.2.3	time	m	m	o	G	See Doc 9880, Part II - 3.1.4.3.10
4.2.4	signed-data	o	m	o	G	
4.2.4.2	content-integrity-check	o	m	o	G	See Doc 9880, Part II - 3.1.4.3.11

M = Mandatory
O = Optional support or optional dynamic use
G = Generated

----------End of references to ISO/IEC ISP 10611-4----------

G.3.2 ATS Message Legal Recording by MTS user

Optionally, the MTS user (UA or MS) may perform ATS Message Legal Recording. See the requirements of the Doc 9880, Part II [10], clause 3.1.3.

H. ANNEX H (NORMATIVE) – REQUIREMENTS OF MESSAGE RETRIEVAL PROTOCOL (P7)

AMHS Addendum to Profile AMH13 – ISO/IEC ISP 10611-5 – MS Access (P7)

H.1 Introduction

This is an addendum to ISO/IEC ISP 10611-Part 5 – AMH13 - MS Access (P7) (the ISP), and should be used in conjunction with the ISP. It contains additional requirements to those specified in the ISP for AMHS User Agents used to originate and retrieve ATS Messages from a Message Store.

Note. – Summary

This profile is very similar to that of the MS Access(94) profile, the difference being that the Base and ISP standards for the MS Access (94) support far more sophisticated manipulation and retrieval of messages. These aspects are of local concern only, and possibly subject to further specification by ANSPs;

There are two parts to P7, an MS part and an MS user part;

The MS part is required to be effectively transparent as far as generation and reception of messages is concerned i.e. the Message Store functions themselves have no impact on the overall operation of ATS Messaging. The MTS user part is also required to be 'transparent', but it is required to generate certain ATS message specific components such as the Message Token, CAAS + XF Address Attributes, and certain body part types;

Also, many of the specifications (i.e. the message operations, apart from Submission and Retrieval and Attribute sets supported by MS-User and MS) are purely local, and are not profiled. Individual ANSPs may have their own preferences (e.g. for BIND credentials and Administration) here;

So, the basic requirements of the ISPs satisfy most of the requirements. However, the P7 profile is enhanced by this addendum in tables A.0.7, A.1.9 A.3.1, A.3.2 and A.3.4 to ensure that the MTS User component and the MTA can transfer, deliver, generate and retrieve several items that are required by for ATS messaging, namely: the Message Token, ia5, general text and File Transfer body parts, IPM(88), DL and S0 functional groups and OR-Address attributes;

Section H.3 indicates further requirements that are mandated for support of the P3 protocol used for ATS messaging Extended Service.

H.2 AFI AMHS Requirements

H.2.1 ISP Conformance

An AMHS UA or MS shall conform to Profile AMH13 – ISO/IEC ISP 10611-5 – MS Access (P7).

H.2.2 Additional Requirements to ISP

The following tables (A.0.7, A.1.9, A.3.1, A.3.2 and A.3.4) specify additional requirements that express restrictions on a set of rows of the AMH13 profile that are referred to using their references in ISO/IEC ISP 10611-5.

----------Begin of references to ISO/IEC ISP 10611-5----------

A.0.7 Statement of profile conformance

Ref	Question	ISP	Doc 9880 Bas/Ext	AFI AMHS	Comments
2	Are all mandatory requirements of any of the following optional functional groups implemented?				
2.1	Distribution List (DL)	o	m/m	m	
2.5	Security (SEC)	o	o/m	o	class(es): S0 – Common Messaging

A.3.1 Content types supported

Ref	Content Type	ISP		Doc 9880 Bas and Ext		AFIAMHS		Comments
		Subm	Retr	Subm	Retr	Subm	Retr	
1	built-in							
1.2	interpersonal-messaging-1984 (2)	o	o	-	-	-	-	not used
1.3	interpersonal-messaging-1988 (22)	o	o	m	m	m	m	

A.3.2 Encoded information types supported

Ref	Encoded Information Type	ISP	Doc 9880		AFI AMHS	Comments
			Submit	Delivery		
		Submit Deliv	Bas/Ext	Bas/Ext	Subm/Del	
1.2	ia5-text (2)	o/m	m/m	m/m	m/m	
2	extended					
2.1						In support for general-text body part as in ISO/IEC 10021-7 B.2
2.1.1	OID {iso(1) standard(0) motis(10021) ipms(7) cs(1) eit-authority(0) 1}	m/m	m/m	m/m	m/m	m in support for of Basic (ISO 646) repertoire o in support for Basic-1(ISO 8859-1) repertoire

Ref	Encoded Information Type	ISP Submit Deliv	Doc 9880 Submit Bas/Ext	Delivery Bas/Ext	AFI AMHS Subm/Del	Comments
2.1.2	OID {iso(1) standard(0) motis(10021) ipms(7) cs(1) eit-authority(0) 6}	m/m	m/m	m/m	m/m	m in support for of Basic (ISO 646) repertoire o in support for Basic-1(ISO 8859-1) repertoire
2.1.3	OID {iso(1) standard(0) motis(10021) ipms(7) cs(1) eit-authority(0) 100}	o/o	o/o	o/o	o/o	o in support for Basic-1(ISO 8859-1) repertoire
2.1.4	OID {joint-iso-itu-i(2) mhs(6) ipms(1) eit(12) file-transfer(0)	o/o	o/o	m/m	m/m	m in support for the File Transfer Body Part

A.3.4 Implementation constraints (a table of ISO/IEC ISP 10611-5)

Suppliers shall state the maximum number of MS users that can be simultaneously supported by an MS implementation.

----------End of references to ISO/IEC ISP 10611-5----------

H.3 Additional MTS User requirements to support AMHS

H.3.1 Dynamic Generation of Message Token by UA for Extended ATS Message Handling Service

AMH13 specifies the static requirements for the Message Token in Table A.1.9/4. The following table specifies the corresponding requirement for dynamic generation of Message Token Fields for MS Users conforming to the S0 Functional Group when generating a secure ATS message. Refer also to Doc 9880, Part II [10] - Table 3-3. Use of Security Elements (Message Token) in the Extended ATS Message Handling Service.

Begin of references to ISO/IEC ISP 10611-5----------

A.1.9 Extension data types

Ref	Element	MTS-User Static Requirement			Dynamic action for secure message	Notes/References
		ISP	Doc 9880 Bas/Ext	AFI AMHS		
4	MessageToken	o	o/m	o	G	
4.1	token-type-identifier	m	m	o	G	See Doc 9880, Part II - 3.1.4.3.6
4.2	asymmetric-token	m	m	o	G	See Doc 9880, Part II - 3.1.4.3.7

Ref	Element	MTS-User Static Requirement			Dynamic action for secure message	Notes/References
		ISP	Doc 9880 Bas/Ext	AFI AMHS		
4.2.1	signature-algorithm-identifier	m	m	o	G	See Doc 9880, Part II - 3.1.4.3.8
4.2.2	name	m	m	o	G	See Doc 9880, Part II - 3.1.4.3.9
4.2.3	time	m	m	o	G	See Doc 9880, Part II - 3.1.4.3.10
4.2.4	signed-data	o	m	o	G	
4.2.4.2	content-integrity-check	o	m	o	G	See Doc 9880, Part II - 3.1.4.3.11

----------End of references to ISO/IEC ISP 10611-5----------

I. ANNEX I (NORMATIVE) – REQUIREMENTS OF MESSAGE RETRIEVAL PROTOCOL (P7) (94) .

AMHS Addendum to Profile AMH15 – ISO/IEC ISP 10611-6 – MS Access-94 (P7)

I.1 Introduction

This is an addendum to ISO/IEC ISP 10611 -Part 6 – AMH15 - MS Access-94 (P7) (the ISP), and should be used in conjunction with the ISP. It contains additional requirements to those specified in the ISP for AMHS User Agents used to originate and retrieve ATS Messages from a '94 Message Store.

Note. – Summary

This profile is very similar to that of the MS Access profile, the difference being that the Base and ISP standards for the MS Access support far more limited facilities for manipulation and retrieval of messages. These aspects are of local concern only, and possibly subject to further specification by ANSPs. They are of no concern to the overall operation of the international ATS messaging service;

There are two parts to P7: an MS part and an MS user part;

The MS part is required to be effectively transparent as far as generation and reception of messages is concerned i.e. the Message Store functions themselves have no impact on the overall operation of ATS Messaging. The MTS user part is also required to be 'transparent', but it is also required to generate certain ATS message specific components such as the Message Token, CAAS + XF Address Attributes, and certain body part types;

Also, many of the specifications (i.e. the message operations, all of the Auto-Actions, apart from Submission and Retrieval and the particular attribute sets for MS user and MS support) are purely local, and are not profiled. Individual ANSPs may have their own preferences here (e.g. for BIND credentials and Administration);

So, the basic requirements of the ISPs satisfy most of the EUR AMHS Requirements. However, the P7 profile is enhanced by this addendum in tables A.0.7, A.2.7.8, A.3.1, A.3.2, A.3.4 and A.3.5 to ensure that the MTS User component and the MTA can transfer, deliver, generate and retrieve several items that are required by for ATS messaging, namely: the Message Token, ia5, general text and File Transfer body parts, IPM(88), DL and S0 functional groups and OR-Address attributes.

I.2 AFI AMHS Requirements

I.2.1 ISP Conformance

AMHS MS (94)s and UAs shall conform to Profile AMH15 – ISO/IEC ISP 10611-6 – MS Access (P7).

I.2.2 Additional Requirements to ISP

The following tables (A.0.7, A.1.9, A.3.1, A.3.2 and A.3.4) specify additional requirements that express restrictions on a set of rows of the AMH15 profile that are referred to using their references in ISO/IEC ISP 10611-6.

----------Begin of references to ISO/IEC ISP 10611-6----------

A.0.7 Statement of profile conformance

Ref	Question	ISP	AMHS Bas/Ext	AFI AMHS	Comments
2	Are all mandatory requirements of any of the following optional functional groups implemented?				
2.1	Distribution List (DL)	o	m/m	m	
2.5	Security (SEC)	o	o/m	o	class(es): S0 Common Messaging

A.3.1 Content types

Ref	Content Type	ISP Subm/ Retr	DOC 9880 Bas and Ext		AFI AMHS	Comments
			Submis-sion	Retrieval		
1	built-in					
1.2	interpersonal-messaging-1984 (2)	o/o	-	-	-	not used
1.3	interpersonal-messaging (22)	o/o	m	m	m	

A.3.2 Encoded information types supported

Ref	Encoded Information Type	ISP Submit Deliv	Doc 9880 Submit Bas/Ext	Delivery Bas/Ext	AFI AMHS Subm/Del	Comments
1.2	ia5-text (2)	o/m	m/m	m/m	m/m	
2	extended					
2.1						In support for general-text body part as in ISO/IEC 10021-7 B.2
2.1.1	OID {iso(1) standard(0) motis(10021) ipms(7) cs(1) eit-authority(0) 1}	m/m	m/m	m/m	m/m	m in support for of Basic (ISO 646) repertoire o in support for Basic-1(ISO 8859-1) repertoire

Ref	Encoded Information Type	ISP Submit Deliv	Doc 9880 Submit Bas/Ext	Delivery Bas/Ext	AFI AMHS Subm/Del	Comments
2.1.2	OID {iso(1) standard(0) motis(10021) ipms(7) cs(1) eit-authority(0) 6}	m/m	m/m	m/m	m/m	m in support for of Basic (ISO 646) repertoire o in support for Basic-1(ISO 8859-1) repertoire
2.1.3	OID {iso(1) standard(0) motis(10021) ipms(7) cs(1) eit-authority(0) 100}	o/o	o/o	o/o	o/o	o in support for Basic-1(ISO 8859-1) repertoire
2.1.4	OID {joint-iso-itu-i(2) mhs(6) ipms(1) eit(12) file-transfer(0)	o/o	o/o	m/m	m/m	m in support for the File Transfer Body Part

A.3.4 Implementation constraints

Suppliers shall state the maximum number of MS Users that can be simultaneously supported by the MS.

----------End of references to ISO/IEC ISP 10611-6----------

I.3 Additional MTA requirements to support Extended AMHS

I.3.1 Dynamic Generation of Message Token by UA for Extended ATS Message Handling Service

AMH15 specifies the static requirements for the Message Token in Table A.1.9/4. The following table specifies the corresponding requirement for dynamic generation of Message Token Fields for MS Users conforming to the S0 Functional Group when generating a secure ATS message. Refer also to Doc 9880, Part II [10] - Table 3-3. Use of Security Elements (Message Token) in the Extended ATS Message Handling Service.

Begin of references to ISO/IEC ISP 10611-6----------

A.1.9 Extension data types

Ref	Element	MTS-User Static Requirement			Dynamic action for secure message	Notes/References
		ISP	Doc 9880 Bas/Ext	AFI AMHS		
4	MessageToken	o	o/m	o	G	
4.1	token-type-identifier	m	m	o	G	See Doc 9880, Part II - 3.1.4.3.6
4.2	asymmetric-token	m	m	o	G	See Doc 9880, Part II - 3.1.4.3.7

Ref	Element	MTS-User Static Requirement			Dynamic action for secure message	Notes/References
		ISP	Doc 9880 Bas/Ext	AFI AMHS		
4.2.1	signature-algorithm-identifier	m	m	o	G	See Doc 9880, Part II - 3.1.4.3.8
4.2.2	name	m	m	o	G	See Doc 9880, Part II - 3.1.4.3.9
4.2.3	time	m	m	o	G	See Doc 9880, Part II - 3.1.4.3.10
4.2.4	signed-data	o	m	o	G	
4.2.4.2	content-integrity-check	o	m	o	G	See Doc 9880, Part II - 3.1.4.3.11

----------End of references to ISO/IEC ISP 10611-6----------

J. ANNEX J (NORMATIVE) – REQUIREMENTS OF OSI UPPER LAYERS FOR AMHS

AMHS Addendum to Profile AMH1n – ISO/IEC ISP 10611-2 Common Messaging Specification of ROSE, RTSE, ACSE, Presentation and Session Protocols for use by MHS

J.1 Introduction

This is an addendum to ISO/IEC ISP 10611-Part 2 – AMH1n – Specification of ROSE, RTSE, ACSE, Presentation and Session Protocols for use by MHS and should be used in conjunction with that ISP. It contains additional requirements to those specified in the ISP for AMHS MTS Users (UAs and MSs), MS Users (UAs) and MTAs for the use of underlying data communications facilities.

Note. – Summary:

The options available for ACSE, Presentation, Session, RTSE and ROSE in 10611-2 are all tightly driven by the selection of the Application Contexts that they support – so, there are few changes to make in this profile;

However, in order to meet the stringent message transit time targets set out within the SPACE project, the Monologue Dialogue Mode has been mandated for the P1 application context in table B.3.2.

J.2 AFI AMHS Requirements

J.2.1 ISP Conformance

AMHS UA, MTA and MS implementations shall conform to ISO/IEC ISP 10611-2 – Requirements of OSI Upper Layers for MHS Support.

J.2.2 Additional Requirements to ISP

The following specify additional AMHS requirements of the implementation that express restrictions on a set of rows of the AMH1n profile that are referred to using their references in ISO/IEC ISP 10611 - 2.

----------Begin of references to ISO/IEC ISP 10611-2----------

Annex A ACSE, Presentation and Session Layers

A.3 Association Control Service Element

There are no changes to the specifications of Association Control Service Element (ACSE).

A.4 Presentation protocol

There are no changes to the specifications of the Presentation Protocol.

A.5 Session protocol

There are no changes to the specifications of the Session Protocol.

Annex B RTSE

B.1 RTSE Protocol

B.3.2 Dialogue mode

Ref	Capability	ISP	AFI AMHS
A.6.2.2	Monologue dialogue-mode	c1	m
A.6.2.2	Two-way alternate dialogue-mode	c2	-

c1 if any P1 application-context is supported then m else –
c2 if any reliable P3 or P7 application-context is supported then m else o

Annex C Remote Operations Service Element (ROSE)

There are no changes to the specifications of the Remote Operations Service Element.

----------End of references to ISO/IEC ISP 10611-2----------

K. ANNEX K (INFORMATIVE) – DIRECTORY INFORMATION SUPPORTING AMHS

AMHS Directory Information - Object Classes and Attributes Profile for AMHS

K.1 Introduction

This indicates the Directory Information which is useful to support of ATS Messaging using AMHS.

Note. – Summary:

This profile indicates the directory information that is useful to support Directory Name Resolution and the mapping of AFTN addresses to and from AMHS addresses.

This profile does not mandate access to the directory to access the information listed in this Annex for a number of reasons. Firstly, it is not clear which functions the directory should support, secondly, it is not clear what access protocols should be used (DAP or LDAP). These issues remain to be clarified. Despite this, the Object Classes and Attribute Types listed in this Annex accurately describe the information requirement, and provide an adequate way of expressing that requirement. This profile therefore assumes that some local mechanisms are available to obtain and input the described information into AMHS systems.

K.2 AMHS Requirements

K.2.1 ISP Conformance

DUAs supporting EUR AMHS may need to have access to the Object Classes, Attribute Types specified in ISO/IEC ISP 10616 1995 (Common Directory Use (Normal)).

DUAs supporting EUR AMHS may need to have access to the Object Classes specified in ISO/IEC ISP 11189 1997 (MHS Use of the Directory).

K.2.2 Additional ATN Object Class Requirements

Table K2.2 lists an additional set of atn Object Classes that a UA or MTA EUR AMHS service might need to have access to. Definitions of these Object Classes are given in Doc 9880, Part IV [12].

Object Class
atn-amhs-user
atn-organizational-unit
atn-organizational-person
atn-organizational-role

Object Class
atn-application-entity
atn-certification-authority
atn-amhs-distribution-list
atn-amhs-user-agent
atn-amhs-gateway
atn-aircraft
atn-facility
atn-amhsMD
atn-idrp-router
atn-dSA
atn-organization

Column: 'Object Class' identifies an object class;

Table K.2.2: atn Object Classes

K.2.3 Additional ATN Attributes Required

Table K.2.3 indicates an additional set of atn Attribute Types that a UA or MTA supporting the EUR AMHS ATS Message Handling Service may need to have access to. Definitions of these Attributes are given in Doc 9880, Part IV [12].

Attribute
atn-AF-address
atn-per-certificate
atn-der-certificate
atn-amhs-direct-access
atn-facility-name
atn-version
atn-amhs-extended-service-support
atn-global-domain-identifier
atn-icao-designator

Attribute
atn-AmhsMD-naming-context
atn-net
atn-amhs-addressing-scheme
atn-amhsMD-naming-context

Table K.2.3: atn Attributes

L. ANNEX L (NORMATIVE) – REQUIREMENTS OF TRANSPORT SERVICES SUPPORTING ATS MESSAGING USE OF RFC 1006/2126 OVER TCP

L.1 Introduction

All of the AMHS OSI Applications (UAs, MTAs, MSs) require provision of the OSI Transport Service, however this Profile requires that they are supported by TCP/IP. In order to use TCP/IP, the Upper Layers shall use an implementation of RFC 1006 or 2126.

Note. – Summary:

The two RFCs 1006 and 2126 are self-contained and are complete specifications of how OSI Upper Layers using the OSI Transport Service are to be mapped on to the underlying TCP service. RFC 1006 specifies a TCP mapping to Ipv4; 2126 specifies a mapping of TCP to Ipv6.

L.2 RFC 1006 and RFC 2126 Requirements

The OSI implementations that conform to this Profile shall support either one or both of the variants listed in Table L.2.

Ref	RFC	AFI AMHS
1	1006	o[1]
2	2126	o[2]

Table L.2: RFC 1006 and 2126 Requirements

[1] if Ipv4 is used then m else –

[2] if Ipv6 is used then m else –

L.3 TCP Requirements

A conforming TCP implementation shall be IP version independent.

M. ANNEX M (NORMATIVE) – REQUIREMENTS OF INTERNET PROTOCOLS IPV4 AND IPV6 .

M.1 Internet Protocol (IP) requirements

Implementations for which conformance to this profile is claimed shall implement either the Ipv4 or the Ipv6 protocol stack or shall implement both.

M.2 IP Addressing

M.2.1 Assignment of IP Addresses

An IP address shall be assigned by the authority implementing this Profile.

M.2.1.1 Traffic Class

A conforming implementation shall not make use of the Traffic Class field.

M.2.1.2 Flow Label

A conforming implementation shall not make use of the Flow Label field by setting this field to zero.

M.2.2 Ipv4 Implementations

Recommendation: It is possible that some implementations are limited to IP version 4 support. In such cases, it is recommended to make use of network address translation protocol translation (NAT-PT) to interwork with remote implementations.

M.3 Network Security

M.3.1 IP Address Validation

The source IP address and TCP port number shall be validated against a local list of valid remote addresses for the system. If an invalid address is detected, the incoming IP packets shall be dropped.

M.3.2 Authentication, Encryption and Integrity

This Profile does not mandate the use of authentication, encryption and integrity services offered by the IPSec standards – RFC 4301

However, use of such techniques and protocols may be bilaterally agreed

N. ANNEX N (NORMATIVE) – OSI ADDRESSING PRINCIPLES AND REGISTERED VALUES FOR AMHS

N.1 Introduction

The following table collects a number of registered name and address values for OSI Upper Layers, Application, TCP ports and IP addresses:

Note. – Summary:

This table simply collects together a number of naming and addressing conventions that are defined in Doc 9880, Part III [11] and various RFCs to provide easy reference, and to ensure that products are capable of using (or pre-specifying) the registered values.

Address Type	UA	MS	MTA
AE-Title	Doc 9880, Part III 2.3.2.2 & 2.3.2.3 [1]	Doc 9880, Part III 2.3.2.2 & 2.3.2.3 [1]	Doc 9880, Part III 2.3.2.2 & 2.3.2.3 [1]
AE Qualifier	AUA(9)	Locally selected	AMS(7)
PSAP	Locally selected	Locally selected	Locally selected
SSAP	Locally selected	Locally selected	Locally selected
TSAP	Locally selected	Locally selected	Locally selected
TCP Port (well-known)	102	102	102
IP Address	Locally selected	Locally selected	Locally selected

Table N.1: Address registrations

[1] AFI AMHS conformant systems shall be capable of being configured to the address values specified in these sections of Doc 9880, Part III [11].

O. ANNEX O (NORMATIVE) – AMHS LOWER-LAYER SECURITY REQUIREMENTS (IPSEC)

O.1 Introduction

Some ANSPs may have concerns for the confidentiality of messages transferred between COM centres. However, use of message confidentiality at the application layer on a per message basis is difficult to apply without partitioning AMHS. For this reason, if a confidentiality requirement exists, then it should be applied at the IP level to all AMHS traffic between international COM Centres, and will need to be administered as a bilateral agreement between those centres.

Note. – Summary:

ANSPs can operate confidentiality encryption to protect messages at the 'link layer' to protect messages during transfer between COM centres, and internally between an ANSPs internal systems.

Recommendation: If a requirement for message confidentiality exists then ANSPs should bilaterally agree to use IPSec (RFC 4301) link-layer encryption together with a bilaterally agreed IPSec cryptographic profile.

P. ANNEX P (NORMATIVE) – AMHS CRYPTOGRAPHIC PROFILE

P.1 Introduction

This is a specification of the use of cryptography used to support the generation and reception of secure ATS Messages over AMHS. It specifies particular values and settings of AMHS protocol elements that reflect the current Security Profile that applies to the Extended ATS, and which directly support the S0 Functional Group specified in Profile AMH1n Common Messaging Part 1 – MHS Service Support. The values and settings specified in this document apply to the following ISPs and their EUR AMHS addenda contained in this document:

ISO/IEC ISP 10611-4 – AMH12 & 14-MS Access (P3)

ISO/IEC ISP 10611-5 – AMH13-MS Access (P7)

ISO/IEC ISP 10611-6 – AMH15-MS Access (P7 94)

Note. – Summary

The S0 FG selects all of the necessary static requirements for S0 – mainly the generation of a Message Token on Origination of a secure ATS Message;

Additionally, the P3 and two P7 Addenda contained in this document specify the Dynamic Requirement for Message Token Generation;

Neither the base standards nor ISPs specify the values (Algorithm types etc.) that should be used to generate and evaluate secured messages. Doc 9880, Part IV does;

Therefore this profile collects together all of the cryptographic specifications that support the S0 Functional Group dynamic generation of the Message Token by UAs in those P3 and P7 protocols;

These specifications are gathered here in a single place to allow easy update, and because they form a single reference used by the P3, P7 and P7(94) ISPs.

P.2 AFI AMHS Requirements

The AFI AMHS Profile does not mandate Security. However, if the S0 functional group is selected, then the provisions of this Annex shall apply.

P.2.1 Secure ATS Message Generation

ATSMHS User Agents that claim conformance to the S0 Functional Group shall generate a Message Token using the following values and settings for generation of a secure message.

Element	Value Setting	References
message token		Doc 9880, Part II - 3.1.4.3.3, 3.1.4.3.4, 3.1.4.3.5
token extension criticality	‘non-critical’	
Token type identifier	Asymmetric	
signature algorithm	ecdsa	Doc 9880, Part IV

Element	Value Setting	References
hash algorithm	sha1	
signature-algorithm-identifier	ecdsa-with-sha1	
name element	MF Address or Directory Name of originator	
time element	Time of message generation	
content-integrity-check		Doc 9880, Part II - 3.1.4.3.11
content-integrity-check criticality	'non-critical'	
content-integrity-check value	signature of the ATN signature scheme's Object Identifier concatenated with the message content	

Table P.2.1: Secure ATS Message Generation

P.2.2 Secure ATS Message evaluation on Reception

On reception of a secure ATS message, an AMHS User Agent that conforms to the S0 Functional Group shall decode and evaluate the messages security elements as specified in Doc 9880, Part II [10], section 3.1.4.3.12, and in Doc 9880, Part IV [12].

Q. ANNEX Q (NORMATIVE) – CONFORMANCE IMPLEMENTATION STATEMENT

Q.1 Conformance Implementation Overview

This Annex provides the PICS Proforma for the AMHS profiles defined in section 6 of this Profile. The Implementation Conformance Statement for an implementation claiming conformance to this profile shall be generated in accordance with the instructions given below.

A conforming implementation shall satisfy the mandatory conformance requirements of the base standards referenced in this profile as well as the applicable Annexes (A to Q) of this Profile.

Q.2 The Role of the PRL and PICS Proformas

The status of this section is informative: it does not constitute a provision of this Part of this Profile.

The objective of presenting the conformance requirements in the tabular form of the PRL and PICS proformas is to provide a check-list of the features which must or may be implemented. The underlying concepts are defined and described in ISO/IEC ISP 9646-1.

A profile combines and selects the options of several base standards in order to fulfil a specific information processing function. In AMHS, each International Standardized Profile (ISP) refers to the Base Standards, and has a PICS proforma, listing the requirements of the standard. Each PRL comprises the subset of the ISPs PICS proforma items that are constrained by the profile, together with the specific profile requirements; it defines answers required on the ISP PICS proformas to conform with the profile. In addition, each PRL will contain PICS-type items which are specific to the profile (at the least, there will be a item testing whether all the required PICS proformas have been correctly completed); these items must be completed together with the referenced ISP's PICS proformas. The completed proformas together constitute a profile Implementation Conformance Statement (ICS).

A claim of conformance to a profile has to be supported by PICS proformas completed in accordance with the PRL. The use of this material will depend on the procurement approach for an AMHS implementation and the particular type of system (UA, MTA or MS) being procured.

Several possible approaches to an AMHS implementation can be imagined :

– In-house implementation by a Member State or Air Navigation Service Provider: the PRL should be used as the basis of the requirements specification and acceptance test specification for the implementation; the completed ICS should be produced as part of the acceptance procedure.

– Implementation of the profile by a contractor: the material will be used and produced as for an in-house implementation, but the contractor should provide the ICS and the need for this must be a contractual requirement.

– Implementation of the profile by a contractor as part of a turn-key or system integration contract: the material will be used and produced as for an in-house implementation, but the contractor must be required to

do this internally as well as providing the completed ICS. Conformance to the profile ensures, for instance, that a supplier working for two organisations cannot introduce its proprietary protocols to meet the AMHS requirement and thus helps to give control to the contracting organisations.

– Integration of off-the-shelf products into a profile implementation in any of the previous cases: the supplier of a product should be required to provide those PICS proformas relevant to the product completed in accordance with the PRL given here and to warrant the conformance of the product with the applicable profile requirements; this PICS can then be forwarded as part of the profile ICS.

Following implementation, the ICS should be maintained as part of the documentation of the implementation; it can be used to predict interoperability with other administrations, and to identify changes that may be needed in moving to different protocols.

Q.3 Instructions for Completing the PICS Proformas

To provide the profile ICS, the PICS proformas for the referenced ISPs shall be completed, together with the additional profile-related PICS items provided in this Annex.

Where this profile refines the features of the base standards and ISPs, the requirements expressed in this PRL shall be applied (as indicated in PRL items with a 'Profile features' column) to constrain the allowable responses in the ISP PICS proformas.

Where this profile makes additional requirements, the response column for such items shall be completed. In this column, each response shall either be selected from the indicated set of responses, or comprise a parameter value or values or range of values as requested.

If a mandatory requirement is not satisfied, exception information must be supplied, by entering a reference X<i>, where <i> is a unique identifier, to an accompanying rationale for the non-compliance.

A possible reason for such an exception is compliance with a pending defect report on a provision of the profile; if the defect report is accepted, the implementation will then be conformant.

Q.4 Conformance Statement for IPM User Agent using P3 Implementations

Q.4.1 Conformance Overview

Supplier	
Contact point for queries about the PICS	
Implementation name/version	
Machine name/version	
Operating system name/version	
Other hardware and operating systems claimed	
System name (if applicable)	
Date of statement	
Have all the mandatory of the sections indicated below including the listed Annexes and other references been implemented? - Section 4.4.1 (IPM UA using P3)	 Yes o
NOTE – Failure to respond 'Yes' to all of these questions indicates a failure of conformance to this profile	
State which PDRs have been implemented in this system	

Table Q.4.1: Identification of IPM UA using P3 System

Q.4.2 Dynamic Conformance Requirements

Does the implementation provide ATS Message Legal Recording?	Yes o
State the maximum message size that can be delivered to the UA	
NOTE – Failure to respond to all of these questions indicates a failure of conformance to this profile	

Table Q.4.2: Dynamic Conformance Requirements

Q.4.3 Transport and Lower Layer Requirements

The Transport and Lower Layer Requirements are to be specified locally by the ANSP.

Q.5 Conformance Statement for IPM User Agent using P7 Implementations

Q.5.1 Conformance Overview

Supplier	
Contact point for queries about the PICS	
Implementation name/version	
Machine name/version	
Operating system name/version	
Other hardware and operating systems claimed	
System name (if applicable)	
Date of statement	
Have all the mandatory of the sections indicated below including the listed Annexes and other references been implemented? - Section 4.4.2 (IPM UA using P7)	Yes o
NOTE – Failure to respond 'Yes' to all of these questions indicates a failure of conformance to this profile	
State which PDRs have been implemented in this system	

Table Q.5.1: Identification of IPM UA using P7 System

Q.5.2 Dynamic Conformance Requirements

Does the implementation provide ATS Message Legal Recording?	Yes o
State the maximum message size that can be delivered to the UA	
NOTE – Failure to respond 'Yes' to all of these questions indicates a failure of conformance to this profile	

Table Q.5.2: Dynamic Conformance Requirements

Q.5.3 Transport and Lower Layer Requirements

The Transport and Lower Layer Requirements are to be specified locally by the ANSP.

Q.6 Conformance Statement for IPM User Agent using P7 (94) Implementations

Q6.1 Conformance Overview

Supplier	
Contact point for queries about the PICS	
Implementation name/version	
Machine name/version	
Operating system name/version	
Other hardware and operating systems claimed	
System name (if applicable)	
Date of statement	
Have all the mandatory of the sections indicated below including the listed Annexes and other references been implemented? - Section 4.4.3 (IPM UA using P7 (94))	Yes o
NOTE – Failure to respond 'Yes' to all of these questions indicates a failure of conformance to this profile	
State which PDRs have been implemented in this system	

Table Q.6.1: Identification of IPM UA using P7 (94)

Q.6.2 Dynamic Conformance Requirements

Does the implementation provide ATS Message Legal Recording?	Yes o
State the maximum message size that can be delivered to the UA	
NOTE – Failure to respond to all of these questions indicates a failure of conformance to this profile	

Table Q.6.2: Dynamic Conformance Requirements

Q.6.3 Transport and Lower Layer Requirements

The Transport and Lower Layer Requirements are to be specified locally by the ANSP.

Q.7 Conformance Statement for IPM UA Co-located with MTA Implementations

Q.7.1 Conformance Overview

Supplier	
Contact point for queries about the PICS	
Implementation name/version	
Machine name/version	
Operating system name/version	
Other hardware and operating systems claimed	
System name (if applicable)	
Date of statement	
Have all the mandatory of the sections indicated below including the listed Annexes and other references been implemented? - Section 4.4.4 (IPM UA co-located with MTA)	Yes o
NOTE – Failure to respond 'Yes' to all of these questions indicates a failure of conformance to this profile	
State which PDRs have been implemented in this system	

Table Q.7.1: Identification of Co-located IPM UA System

Q.7.2 Dynamic Conformance Requirements

Does the implementation provide ATS Message Legal Recording?	Yes o
State whether any of the Elements of Service for the EUR AMHS IPM and MTS Messaging Services cannot be accessed by the user.	
State whether any of the Extended ATS Elements of Service cannot be accessed by the user.	
State the maximum message size that can be delivered to the UA	
NOTE – Failure to respond to all of these questions indicates a failure of conformance to this profile	

Table Q.7.2: Dynamic Conformance Requirements

Q.7.3 Transport and Lower Layer Requirements

The Transport and Lower Layer Requirements are to be specified locally by the ANSP.

Q.8 Conformance Statement for Message Transfer Agents

Q.8.1 Conformance Overview

Supplier	
Contact point for queries about the PICS	
Implementation name/version	
Machine name/version	
Operating system name/version	
Other hardware and operating systems claimed	
System name (if applicable)	
Date of statement	
Have all the mandatory of the sections indicated below including the listed Annexes and other references been implemented? - Section 4.5 (MTA Requirements)	Yes o
NOTE – Failure to respond 'Yes' to all of these questions indicates a failure of conformance to this profile	
State which PDRs have been implemented in this system	

Table Q.8.1: Identification of MTA System

Q.8.2 Dynamic Conformance Requirements

Does the implementation provide ATS Message Legal Recording?	Yes o
State the number of simultaneous P1 Associations that the MTA can maintain	
State the MTA Transit time per message (See Annex F – A.3.5.2)	
State the maximum message size that the MTA can accept, switch and forward in octets	
Are the TCP port values to service incoming connection establishments configurable?	Yes o
Is the implementation IP version independent?	Yes o
Are the IP addresses of local and remote implementations configurable?	Yes o
Does the implementation make use of Network Address Translation - Protocol Translation (NAT-PT)	Yes o No o
NOTE – Failure to respond 'Yes' to all of these questions indicates a failure of conformance to this profile	

Table Q.8.2: Dynamic Conformance Requirements

Q.8.3 Upper Layer Requirements

Does the supplied RTSE support the Monologue Dialogue Mode?	Yes o No o

Table Q.8.3: RTSE Mode

Q.8.4 Lower Layer Requirements

Is the Transport Service provided by either RFC 1006 or RFC 2126?	Yes o
Is RFC 1006 supported?	Yes o
Is RFC 2126 supported	Yes o
Does the TCP implementation comply to RFC1122 section 4?	Yes o
Are at least 100 simultaneous TCP connections supported for the purpose of AMHS P1 Associations?	Yes o
NOTE – Failure to respond to all of these questions indicates a failure of conformance to this profile	

Table Q.8.4.1: Transport and TCP Layers

Does the IP implementation comply to RFC2460?	Yes o
Are remote IP addresses validated during connection establishment ?	Yes o
NOTE – Failure to respond to all of these questions indicates a failure of conformance to this profile	

Table Q.8.4.2: Network Layer

Does the IP implementation comply to RFC1122 section 2?	Yes o
NOTE – Failure to respond to all of these questions indicates a failure of conformance to this profile	

Table Q.8.4.3: Data Link Layer

Q.9 Conformance Statement for Message Store implementations

Q.9.1 Conformance Overview

Supplier	
Contact point for queries about the PICS	
Implementation name/version	
Machine name/version	
Operating system name/version	
Other hardware and operating systems claimed	
System name (if applicable)	
Date of statement	
Have all the mandatory of the sections indicated below including the listed Annexes and other references been implemented? - Section 4.6 (Message Store)	Yes o
NOTE – Failure to respond 'Yes' to all of these questions indicates a failure of conformance to this profile	
State which PDRs have been implemented in this system	

Table Q.9.1: Identification of MS System

Q9.2 Dynamic Conformance Requirements

Does the implementation provide ATS Message Legal Recording?	Yes o
State the maximum size of messages that can be delivered to the MS	
NOTE – Failure to respond to all of these questions indicates a failure of conformance to this profile	

Table Q.9.2: Dynamic Conformance Requirements

Q.9.3 Transport and Lower Layer Requirements

The Transport and Lower Layer Requirements are to be specified locally by the ANSP.

Q.10 Conformance Statement for MS (94) Implementations

Q.10.1 Conformance Overview

Supplier	
Contact point for queries about the PICS	
Implementation name/version	
Machine name/version	
Operating system name/version	
Other hardware and operating systems claimed	
System name (if applicable)	
Date of statement	
Have all the mandatory of the sections indicated below including the listed Annexes and other references been implemented? - Section 4.7 (Message Store (94))	Yes o
NOTE – Failure to respond 'Yes' to all of these questions indicates a failure of conformance to this profile	
State which PDRs have been implemented in this system	

Table Q.10.1: Identification of MS (94) System

Q.10.2 Dynamic Conformance Requirements

Does the implementation provide ATS Message Legal Recording?	Yes o
State the maximum number of MTS Access (94) Associations that can be simultaneously supported by the Message Store	
NOTE – Failure to respond to all of these questions indicates a failure of conformance to this profile	

Table Q.10.2: Dynamic Conformance Requirements

Q.10.3 Transport and Lower Layer Requirements

The Transport and Lower Layer Requirements are to be specified locally by the ANSP.

R. ANNEX R (INFORMATIVE) – REFERENCES ACROSS EDITIONS OF ISO/IEC ISPS

This document uses references of ISO/IEC ISPs as found in Edition 3 of each of these documents, published in 2003.

These references have evolved since Edition 1 of these documents was published in 1994 or 1995.

The ICAO Doc 9880, Part II [10], makes use of references to Edition 1 of the ISPs as far as the specification of the Basic ATS Message Handling Service is concerned.

The following tables provide the mapping between references of sections and items in Edition 1 (used in Doc 9880, Part II) and in Edition 3 (used in this document).

The mapping is limited to the sections and items used in Doc 9880, Part II [10] and/or in this document, and that have been subject to renumbering through the ISP Edition process. The numbering hierarchy is also provided, even if not renumbered, to enable unambiguous localization of the amended sections and items.

ISO/IEC ISP 10611-6 and of ISO/IEC ISP 12062-6 are both related to MS 94 Access (P7) and their edition dates are different from other parts of the ISPs. Their Edition 1 was published in 1997 only. Therefore the relevant tables below provide the mapping between references of items in Edition 1 and in Edition 2, which was published in 2003 at the same time as Edition 3 of other parts of this multi-part ISO/IEC ISP.

Amended references are identified using bold and italics characters.

ISO/IEC ISP 10611-3

ISP Edition 1 ref	ISP Edition 3 ref	Name of section/item
A.1	A.1	Basic requirements
A.1.4.2	A.1.4.2	Message Transfer
1	1	Message Transfer Envelope
1.1	1.1	(per message fields)
1.1.11	1.1.11	extensions
-	***1.1.11.13***	certificate-selectors
-	***1.1.11.14***	multiple-originator-certificates
-	***1.1.11.15***	dl-exempted-recipients
-	***1.1.11.16***	Private Extensions
A.1.4.3	A.1.4.3	Report Transfer
1	1	Report Transfer Envelope
1.4	1.4	extensions

ISP Edition 1 ref	ISP Edition 3 ref	Name of section/item
1.4.2	***1.4.3***	originator-and-DL-expansion-history
1.4.3	***1.4.4***	reporting-DL-name
1.4.4	***1.4.5***	reporting-MTA-certificate
1.4.5	***1.4.6***	report-origin-authentication-check
1.4.6	***1.4.7***	internal-trace-information

ISO/IEC ISP 10611-4

ISP Edition 1 ref	ISP Edition 3 ref	Name of section/item
A.2	A.2	Optional functional groups
A.2.7	A.2.7	Security (SEC)
A.2.7.7	***A.2.7.8***	Extension data types

ISO/IEC ISP 10611-5

ISP Edition 1 ref	ISP Edition 3 ref	Name of section/item
A.0	A.0	Identification of the implementation
A.0.7	A.0.7	Statement of profile conformance
2	2	Are all mandatory requirements of any of the following optional functional groups implemented?
-	***2.1***	Distribution List (DL)
2.4	***2.5***	Security (SEC)

ISO/IEC ISP 10611-6

ISP Edition 1 ref	ISP Edition 2 ref	Name of section/item
(published 1997)	**(published 2003)**	
A.0	A.0	Identification of the implementation
A.0.7	A.0.7	Statement of profile conformance
2	2	Are all mandatory requirements of any of the following optional functional groups implemented?
-	***2.1***	Distribution List (DL)
2.4	***2.5***	Security (SEC)

ISO/IEC ISP 12062-2

ISP Edition 1 ref	ISP Edition 3 ref	Name of section/item
A.0	A.0	Identification of the implementation
A.0.6	A.0.6	Statement of profile conformance
2	2	Are all mandatory requirements of any of the following optional functional groups implemented?
2.7	***2.2***	IPM Security (SEC)
-	***2.5***	Business Class (BC)
A.1	A.1	Basic requirements
A.1.2	A.1.2	IPM heading fields
17	17	extensions
-	***17.4***	body-part-signatures
-	***17.5***	ipm-security-label
-	***17.6***	authorization-time
-	***17.7***	circulation-list-recipients
-	***17.8***	distribution-codes
-	***17.9***	extended-subject
-	***17.10***	information-category
-	***17.11***	manual-handling-instructions
-	***17.12***	originators-reference
-	***17.13***	precedence-policy-identifier
A.1.5	A.1.5	Common Data Types
1	1	Recipient Specifier
1.4	1.4	recipient-extensions
-	***1.4.2***	circulation-list-indicator
-	***1.4.3***	precedence

ISO/IEC ISP 12062-5

ISP Edition 1 ref	ISP Edition 3 ref	Name of section/item
A.0	A.0	Identification of the implementation
A.0.7	A.0.7	Statement of profile conformance
3	3	Are all mandatory requirements of any of the following optional functional groups implemented?
-	***3.2***	IPM Distribution List (DL)
3.6	***3.7***	IPM Security (SEC)
-	***3.9***	Business Class (BC)
-	***A.1***	Basic requirements
A.1.12	A.1.12	IPM-specific attributes
A.1.12.1	A.1.12.1	Extended body part attribute support
1	1	ia5-text-body-parts
-	***9***	bilaterally-defined-body-parts
3	***11***	general-text-body-parts
B.2	B.2	Optional functional groups
B.2.6	***B.2.7***	IPM Security (SEC)
-	***B.2.9***	Business Class (BC)

ISO/IEC ISP 12062-6

ISP Edition 1 ref	ISP Edition 2 ref	Name of section/item
(published 1997)	**(published 2003)**	
A.0	A.0	Identification of the implementation
A.0.7	A.0.7	Statement of profile conformance
3	3	Are all mandatory requirements of any of the following optional functional groups implemented?
-	***3.2***	IPM Distribution List (DL)

ISP Edition 1 ref	ISP Edition 2 ref	Name of section/item
3.6	***3.7***	IPM Security (SEC)
-	***3.13***	Business Class (BC)
-	***A.1***	Basic requirements
B.2	B.2	Optional functional groups
B.2.6	***B.2.7***	IPM Security (SEC)
-	***B.2.13***	Business Class (BC)

END of Appendix B