

**EUROCONTROL SPECIFICATION  
on the  
Air Traffic Services Message  
Handling System (AMHS)**

**SPECIFICATION DOCUMENT IDENTIFIER: EUROCONTROL-SPEC-0136**

<b>Edition Number</b>	<b>:</b>	<b>2.0</b>
<b>Edition Date</b>	<b>:</b>	<b>18/09/2009</b>
<b>Status</b>	<b>:</b>	<b>Released</b>
<b>Intended for</b>	<b>:</b>	<b>General Public</b>
<b>Category</b>	<b>:</b>	<b>EUROCONTROL Specification</b>

## DOCUMENT CHARACTERISTICS

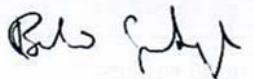

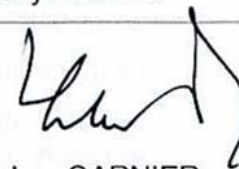

TITLE		
<h3 style="margin: 0;">EUROCONTROL Specification on the Air Traffic Services Message Handling System (AMHS)</h3>		
<b>Document Identifier</b>	<b>Edition Number:</b>	2.0
EUROCONTROL-SPEC-0136	<b>Edition Date:</b>	18/09/2009
<b>Abstract</b>		
<p>This document is the EUROCONTROL Specification, developed under the EUROCONTROL Regulatory and Advisory Framework (ERAF), for the ATS Message Handling System (AMHS) as it applies to the EATMN. The objective is to define precise means of compliance to the essential requirements of the interoperability Regulation to ensure interoperability of AMHS systems and constituents in the framework of the Single European Sky.</p> <p>Implementations that comply with the mandatory provisions of this specification will be compliant to the essential requirements of the interoperability Regulation.</p>		
<b>Keywords</b>		
AMHS SES	Specification	Interoperability
<b>Contact Person(s)</b>	<b>Tel</b>	<b>Unit</b>
Boleslaw Gasztych	+32 2 729 3153	CND/COE/CN/CO

DOCUMENT STATUS AND TYPE					
Status		Intended for		Category	
Working Draft	<input type="checkbox"/>	General Public	<input checked="" type="checkbox"/>	EUROCONTROL Rule	<input type="checkbox"/>
Draft	<input type="checkbox"/>	Restricted EUROCONTROL	<input type="checkbox"/>	EUROCONTROL Specification	<input checked="" type="checkbox"/>
Proposed Issue	<input type="checkbox"/>			EUROCONTROL Guideline	<input type="checkbox"/>
Released Issue	<input checked="" type="checkbox"/>				

ELECTRONIC SOURCE		
Path:		
Host System	Software	Size
Windows_XP	Microsoft Word 2002 SP3	3.6 MB

## DOCUMENT APPROVAL

The following table identifies all management authorities who have successively approved the present issue of this document.

AUTHORITY	NAME AND SIGNATURE	DATE
EC Mandate Manager CND/COE/CNS/COM	 Mr Boleslaw GASZTYCH	09.10.09
Manager CND/COE/CNS/COM	 My Jacky POUZET	09.10.09.
CND Deputy Director for Single European Sky Implementation	 Mr Jean-Luc GARNIER	09/10/09
On behalf of the Director General, by special delegation  Director CND	 Mr Bo REDEBORN	9/10/09

## DOCUMENT CHANGE RECORD

The following table records the complete history of the successive editions of the present document.

EDITION NUMBER	EDITION DATE	INFOCENTRE REFERENCE	REASON FOR CHANGE	PAGES AFFECTED
0.1	16/01/08		Initial outline	All
0.2	25/01/08		Detail added	All
0.3	26/02/08		Further evolution. Input to Drafting Group	All
0.4	01/04/08		Further evolution. Comments from drafting group 29/02/08.	All
0.5	13/06/08		Draft for Review Group	All
0.6	24/10/08		Updated after informal stakeholder review. Annex A split into 2 – Basic & Extended	All
1.0	08/12/08		Updated after informal stakeholder review. Input to formal consultation.	All
1.1	27/07/09		Updated after ENPRM-09/001 formal consultation.	All
2.0	18/09/09		Released Issue	1, 3, 4, 48

# CONTENTS

<b>1. INTRODUCTION.....</b>	<b>2</b>
1.1 Document Structure .....	2
1.2 Purpose .....	3
1.3 Background Context.....	4
1.4 Scope .....	6
1.5 Document Status.....	8
1.6 Applicability .....	9
1.7 Conventions .....	10
1.8 Abbreviations and Definitions .....	11
1.9 Interoperability Target .....	17
1.10 Responsible Unit .....	22
<b>2. AMHS INTEROPERABILITY – BASIC ATSMHS.....</b>	<b>23</b>
2.1 General.....	23
2.2 Standards Baseline .....	23
2.3 Network Support .....	24
2.4 Safety and Performance Requirements.....	24
2.5 Message Transfer Service Interoperability .....	25
2.6 End to End Interoperability of Direct AMHS Users .....	26
2.7 Interoperability between AFTN and AMHS.....	26
2.8 Ground Recording of Messages .....	26
2.9 Naming and Addressing.....	27
2.10 Operational Procedures .....	27
2.11 Interoperability with Military Message Handling Systems.....	27
2.12 Interoperability with Systems External to EATMN .....	28
<b>3. EXTENDED ATSMHS.....</b>	<b>30</b>
3.1 General.....	30
3.2 Standards Baseline .....	30
3.3 Extended ATSMHS Functionality.....	30
3.4 End to End Interoperability of Direct AMHS Users .....	32
3.5 Naming and Addressing.....	33
<b>4. USE OF DIRECTORY.....</b>	<b>34</b>
4.1 General.....	34
4.2 Directory Architecture.....	34

4.3	Directory System Protocols.....	37
4.4	Directory Access .....	38
4.5	Directory Schema.....	38
4.6	Versioning and Data Life Cycle.....	41
4.7	Use of Directory to determine AMHS Recipient Capabilities .....	42
<b>5.</b>	<b>AMHS SECURITY .....</b>	<b>43</b>
5.1	General.....	43
5.2	AMHS Security Framework.....	44
5.3	Public Key Infrastructure .....	45
<b>6.</b>	<b>ADDITIONAL AMHS REQUIREMENTS.....</b>	<b>46</b>
6.1	Testing and Verification.....	46
<b>7.</b>	<b>TRANSITION / COEXISTENCE ISSUES.....</b>	<b>47</b>
7.1	AFTN to AMHS Transition.....	47
7.2	Basic ATSMHS to Extended ATSMHS Transition .....	48
7.3	Deployment of Directory.....	48
<b>8.</b>	<b>TRACEABILITY TO REGULATORY PROVISIONS.....</b>	<b>49</b>
8.1	Implementation Conformance Statements.....	49
8.2	Traceability to SES Essential Requirements .....	49
<b>9.</b>	<b>DOCUMENT UPDATE PROCEDURES.....</b>	<b>51</b>
<b>10.</b>	<b>LIST OF REFERENCES .....</b>	<b>53</b>
10.1	Description of References.....	53
10.2	Primary References .....	53
10.3	Associated References .....	55
	<b>ANNEX A - BASIC SERVICE .....</b>	<b>A-1</b>
	<b>ANNEX B - EXTENDED SERVICE .....</b>	<b>B-1</b>
	<b>ANNEX C - DIRECTORY REQUIREMENTS .....</b>	<b>C-1</b>
	<b>ANNEX D – AMHS SECURITY.....</b>	<b>D-1</b>
	<b>APPENDIX 1 – Traceability Matrix between SES Essential Requirements and EUROCONTROL Specification</b>	
	<b>APPENDIX 2 – Current Editions of Referenced Standards</b>	

## List of Tables

Table 1: Definition of ATSMHS subsets.....	31
--	----

## List of Figures

Figure 1: Relationship to other documents .....	8
Figure 2: Requirement identifier format .....	11
Figure 3: AMHS Interoperability Target .....	18
Figure 4: AMHS Interoperability Target (transitional phase) .....	20
Figure 5: COM Centre perspective .....	22
Figure 6: Dual communications stack at Regional boundary .....	29
Figure 7: SEC FG in ISPs vs. Extended ATSMHS.....	32
Figure 8: General Directory Architecture .....	35
Figure 9: Initial Directory architecture .....	36
Figure 10: Future Directory architecture .....	37
Figure 11: DIT Structure .....	39
Figure 12: Global AMHS Architecture including CA.....	45





## **EXECUTIVE SUMMARY**

This document is the EUROCONTROL Specification for the Air Traffic Services Message Handling System (AMHS) in Europe. It has been developed under the EUROCONTROL Regulatory and Advisory Framework (ERAF). The objective is to define precise means of compliance to the essential requirements of the interoperability Regulation to ensure interoperability of AMHS systems and constituents in the framework of the Single European Sky (SES).

This EUROCONTROL Specification refines and augments the detailed technical specifications for AMHS in ICAO Annex 10 and associated ICAO technical manuals, for deployment in the European Air Traffic Management Network (EATMN). The goal is to enable EATMN-wide support of a specific profile of the Extended level of service of the ATS Message Handling Service (ATSMHS), as defined by ICAO. This includes:

- a) support for binary information transfer,
- b) operation over a network infrastructure based on the internet protocol (IP),
- c) use of standard message heading extensions to convey Air Traffic Services (ATS) header information,
- d) use of directory functionality to enhance interoperability,
- e) migration to the use of digitally signed secure messages at a future date if required.

An initial transition step supporting migration from the AFTN to the Basic ATSMHS level of service is also foreseen.

The provisions of this EUROCONTROL Specification are applicable to air navigation service providers (ANSPs) in EU Member States. Specifically, the provisions apply to the parts of an ANSP's organisation responsible for providing, directly or by outsourcing, data messaging services to end users both within and between States.

This EUROCONTROL Specification is organised as a number of chapters and annexes. Compliance with this EUROCONTROL Specification is achieved once implementations comply with all requirements of the normative Annexes. After being referenced in the Official Journal of the European Union as a Community specification, full compliance to this EUROCONTROL Specification gives a formal presumption of conformity with the essential requirements and regulatory provisions identified in Chapter 8 and Appendix 1.

The use of Community specifications to demonstrate conformity with the essential requirements and regulatory provisions is voluntary. ANSPs may choose to use other specifications, or part of this EUROCONTROL Specification. However, ANSPs would then be required to demonstrate compliance with the essential requirements and regulatory provisions in agreement with their national supervisory authority.

## 1. INTRODUCTION

### 1.1 Document Structure

1.1.1 This EUROCONTROL Specification is organised as a number of Chapters and Annexes. The chapters in the main body of the document provide contextual guidance and explanatory material and point to the annexes which contain the normative requirements. The main body is structured as follows:

- The present Chapter includes introductory material describing the purpose and scope of the EUROCONTROL Specification, its structure, and a description of the document conventions, abbreviations, definitions and the interoperability target.
- Chapter 2 describes the basic level of interoperability for the Air Traffic Services Message Handling Service (ATSMHS) in Europe.
- Chapter 3 contains explanatory material concerning the Extended ATSMHS functionality.
- Chapter 4 describes the introduction of Directory systems and procedures.
- Chapter 5 describes the Security mechanisms and procedures to support the Extended ATSMHS.
- Chapter 6 describes additional requirements relating to implementation options, testing and validation.
- Chapter 7 describes some of the transition and coexistence issues.
- Chapter 8 addresses traceability between the means of compliance in this EUROCONTROL Specification and Single European Sky (SES) essential requirements.
- Chapter 9 describes the procedures for maintaining and updating this EUROCONTROL Specification.
- Chapter 10 contains a list of documents which are referenced from the main body and annexes by means of reference numbers contained in square brackets.

1.1.2 Detailed interoperability and compliance requirements are specified in Annexes, which form an integral part of this EUROCONTROL Specification:

- Annex A (normative) contains detailed requirements for the Air Traffic Services (ATS) Message Handling functionality at the level of the Basic ATSMHS. It identifies the systems that are deployed in order to provide

those services, the system level requirements, and the external standards and documents applicable to each system. For each such standard, the baseline version is identified in Chapter 10, and any additional requirements are specified.

- Annex B (normative) contains detailed requirements for the ATS Message Handling functionality at the Extended ATSMHS level of service, requiring support of Functional Groups (FG) for the Basic ATSMHS (Basic FG), use of file transfer body parts for binary data exchange (FTBP FG), use of interpersonal messaging heading extensions (IHE FG) and use of Directory (DIR FG). Support of AMHS Security (SEC FG) is foreseen in the future.
- Annex C (normative) contains detailed requirements for Directory systems to support the DIR FG of the Extended ATSMHS.
- Annex D (informative) indicates high level provisions for security mechanisms that would be needed to support the SEC FG of the Extended ATSMHS (see Note 2).

*Note 1. The actual requirements are therefore specified in normative Annexes, with a separate Annex for each main area of functionality. This could facilitate a step-wise implementation approach to full compliance with this EUROCONTROL Specification (see 1.5.6 below).*

*Note 2. It is recognised that the provision of AMHS Security services is not as advanced as other elements of the Extended ATSMHS, and still requires a number of technical and procedural issues to be resolved in a suitable forum. For that reason, the specifications in Annex D are considered as advisory indications of the evolutionary direction.*

1.1.3 Compliance requirements are provided where possible in the form of protocol implementation conformance statement (PICS) tables giving a detailed statement of functional and protocol compliancy. These tables are generally contained in external standards referenced from this EUROCONTROL Specification.

## 1.2 Purpose

1.2.1 This EUROCONTROL Specification on the Air Traffic Services Message Handling System (AMHS) is developed to complement the Single European Sky (SES) interoperability Regulation No 552/2004 [1] in the area of ground-ground ATS communications.

1.2.2 This EUROCONTROL Specification is organised as a number of chapters and normative annexes. Therefore compliance with this EUROCONTROL Specification is achieved once implementations comply with all requirements of the normative Annexes. After being referenced in the Official Journal of the European Union as a Community specification, full compliance to this EUROCONTROL Specification gives a formal presumption of conformity with

the essential requirements and regulatory provisions identified in Chapter 8 and Appendix 1.

- 1.2.3 The use of Community specifications to demonstrate conformity with the essential requirements and regulatory provisions is voluntary. ANSPs may choose to use other specifications, or part of this EUROCONTROL Specification. However, ANSPs would then be required to demonstrate compliance with the essential requirements and regulatory provisions in agreement with their national supervisory authority.
- 1.2.4 To ensure the interoperability and the seamless operations of the ATSMHS in the European Air Traffic Management Network (EATMN) in terms of the SES interoperability Regulation [1], this EUROCONTROL Specification is intended to augment the relevant technical standards with further standardisation materials directly applicable to the EATMN.
- 1.2.5 This EUROCONTROL Specification on AMHS supports the co-ordinated introduction of new concepts of operations in the EATMN based on high capacity, secure, reliable ground-ground communications.

### **1.3 Background Context**

- 1.3.1 The exchange of ATS messages, as part of the Aeronautical Fixed Service (AFS) defined in ICAO Annex 10 Volume II [3] is an essential function to the safety of air navigation and to the regular, efficient and economical operation of ATS provision.
- 1.3.2 The Aeronautical Fixed Telecommunications Network (AFTN), complemented in Europe by the Common ICAO Data Interchange Network (CIDIN), has provided an effective store-and-forward messaging service for the conveyance of text messages, using character-oriented procedures, for many years. However AFTN / CIDIN technology is now becoming obsolescent, and is not sufficiently flexible to support messaging functions found in modern messaging systems (such as transfer of binary information).
- 1.3.3 It is intended that existing AFTN and CIDIN users and systems will transition to the architecture of the Aeronautical Telecommunication Network (ATN), and this is enabled in part by the ATSMHS application, which has been defined by ICAO to replace the AFTN telegraphic style of working with a modern store-and-forward Message Handling System based on international Standards.
- 1.3.4 Standards and Recommended Practices (SARPs) for the ATSMHS application are specified in ICAO Annex 10 to the Convention on International Civil Aviation (Annex 10 Volume II [3], Chapter 4.6 and Annex 10 Volume III, Part I [26], Chapter 3.5.3). These SARPs refer to detailed specifications in the relevant technical Manual (ICAO Doc 9705, superseded by ICAO Doc 9880 Part IIB [5]).
- 1.3.5 The technical provisions in ICAO Doc 9880 Part IIB [5] define two fundamental levels of service within the ATSMHS; the Basic ATSMHS and the Extended

ATSMHS. Additionally, ICAO Doc 9880 (Part IIB, section 3.4) outlines various subsets of the Extended ATSMHS, to which conformance can be claimed.

- 1.3.6 The Basic ATSMHS performs an operational role similar to the AFTN with a few enhancements, while the Extended ATSMHS provides more advanced features. The Extended level of service includes the Basic level of service capability; in this way it is ensured that users with Extended Service capabilities can interoperate, at a basic level, with users having Basic Service capabilities and vice-versa.
- 1.3.7 The ATSMHS is provided by a set of ATN End Systems, which collectively comprise the *ATS Message Handling System* (AMHS), and which co-operate to provide users (human or automated) with a data communication service. The AMHS network is composed of interconnected *ATS Message Servers* that perform message switching at the application layer (Layer 7 in the basic reference model for open systems interconnection (OSI)). Direct users connect to *ATS Message Servers* by means of *ATS Message User Agents*. An *ATS Message User Agent* supporting the Extended level of service will use the Basic level of service to allow communication with users who only support the Basic ATSMHS. To support the transition from AFTN, *AFTN/AMHS Gateways* provide interfaces between the AMHS and the AFTN. The AMHS network makes use of an underlying network infrastructure that allows data interchange to be performed.
- 1.3.8 Implementation of the Extended ATSMHS implies the existence of various support functions, which are not necessarily exclusively dedicated to messaging. These include Directory support and (if secure messaging is implemented) public key management functions.
- 1.3.9 Communication systems and procedures for ground-to-ground communications in the EATMN are required<sup>1</sup> to support the implementation of advanced, agreed and validated concepts of operation for all phases of flight.
- 1.3.10 The establishment of common interoperability and performance levels once AMHS is deployed across the EATMN will contribute to the achievement of seamless operations by specifying:
- Coherent service levels and operational concepts throughout the applicable area;
  - A communications system supporting a seamless relationship between ground-based systems, so that a service is not disrupted by breaks in coverage or wide variations in quality of service.
- 1.3.11 The ATSMHS offers a communication service to ground systems and their constituents supporting new, agreed and validated concepts of operation which must be designed, built, maintained and operated, using appropriate and validated procedures, in such a way as to be interoperable in terms of timely sharing of correct and consistent information.

---

<sup>1</sup> SES interoperability Regulation [1], Annex II, Part B, paragraph 4.2.

- 1.3.12 The requirement to implement ICAO specifications for aeronautical message handling is reflected in the EUROCONTROL ATM Strategy for the Years 2000+ [44], and specifically in the European Convergence and Implementation Plan (ECIP) [37], though Objective COM05<sup>2</sup>, which states:
- "COM05: Migrate from AFTN/CIDIN to AMHS for international communications:*
- "Implement the international ATS Message Handling Service standardised by ICAO as an X.400-based replacement for the existing AFTN/CIDIN messaging systems that are becoming obsolete and might be unable to support future messaging requirements. ANSPs have the choice to either upgrade their existing COM centre with AMHS capability (as done already by Spain) or implement an AMHS/AFTN gateway in front of their existing switch."*
- 1.3.13 In terms of the ATM Master Plan [46], AMHS is recognised as part of Capability Level 0 deployment for the interconnection of stakeholder's systems.
- 1.3.14 It is therefore likely that ATSMHS functionality will be a fundamental requirement in any procurement of a system that supports aeronautical message handling. This is particularly true for systems that will communicate across national borders.

## **1.4 Scope**

- 1.4.1 This EUROCONTROL Specification defines detailed requirements, explanatory materials and conformity assessment materials providing means of compliance (MOC) associated with the SES interoperability Regulation [1].
- 1.4.2 The scope of this document covers the Basic and Extended levels of the ATSMHS. Specifically, support for functional groups Basic, FTBP, IHE and DIR is specified. Functional group SEC is outlined as an indication of future requirements.
- 1.4.3 This EUROCONTROL Specification is intended to provide a definitive statement on the compliancy requirements for systems and procedures. As such, for each external standard, it identifies the baseline version of that standard and the changes to those standards that are required. Each identified change that is incorporated into this specification includes the original reference.
- 1.4.4 The specification applies to the following EATMN systems:
- Ground communication and display systems, including user interfaces and end systems concerned with message submission, transfer, delivery and (in the case of AFTN interworking) conversion;

---

<sup>2</sup> This ECIP objective will be replaced by a SESAR-related ESSIP objective covering the same topic.

- Ground data logging and recording systems, which, in general, will be an integral part of the communication subsystems.

1.4.5 Compliance with this EUROCONTROL Specification would be mandated in a call for tender for an AMHS End System. However, this EUROCONTROL Specification is not intended to be a complete system specification sufficient for procurement purposes.

1.4.6 The specification includes requirements applicable to operational procedures in the following areas:

- Procedures for the operation and introduction of the ATSMHS, including coexistence with, and transition from, AFTN, and migration from Basic to Extended ATSMHS;
- Procedures for the management of names and addresses and other information required for the operation of the AMHS, such as information on address conversion, user capabilities, etc.

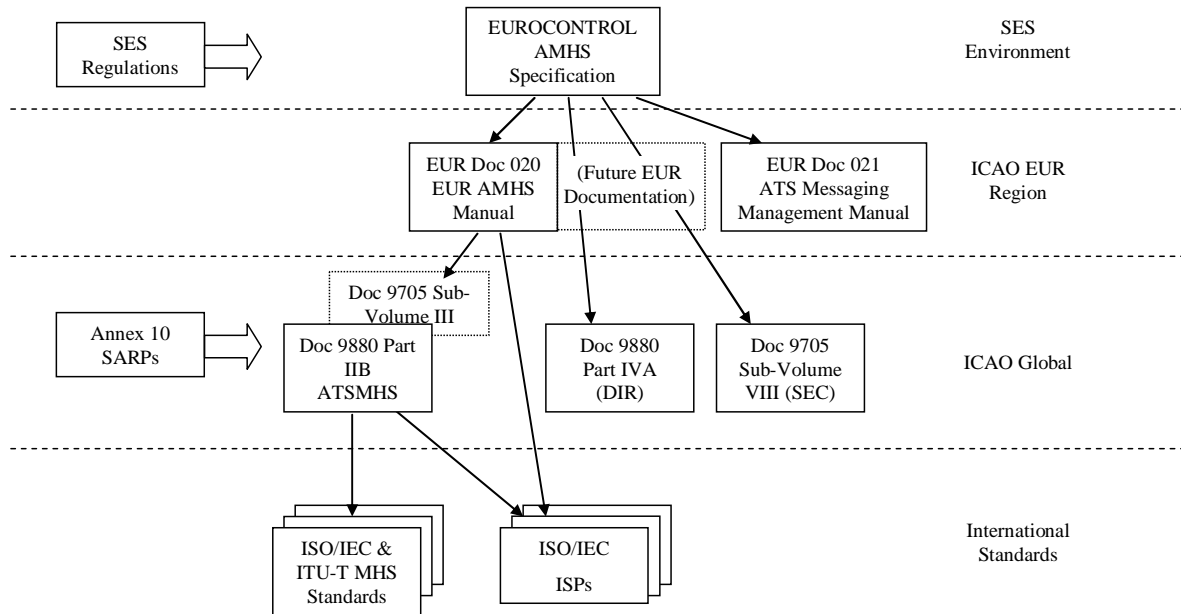
1.4.7 Topics addressed by this EUROCONTROL Specification include:

- The Basic ATSMHS and transition to Extended ATSMHS, including Safety and Security standards, and Directory services;
- The interoperability aspects between implementations of the Basic ATSMHS, with its functional components, and implementations conforming to the provisions of this EUROCONTROL Specification;
- The interoperability aspects of AFTN/AMHS gateways within the transition phase from AFTN to AMHS;
- The tests and verifications of compliance with the provisions of this EUROCONTROL Specification.

1.4.8 This EUROCONTROL Specification aims to be consistent with relevant ICAO and European standards, and includes mechanisms to ensure an efficient process of update to enable ongoing consistency.

EUROCONTROL SPECIFICATION  
on the  
Air Traffic Services Message Handling System (AMHS)

---



**Figure 1: Relationship to other documents**

1.4.9 The relationship of this EUROCONTROL Specification to other documents is summarised in Figure 1. This shows that the EUROCONTROL Specification refines the SES Essential Requirements in the AMHS area and refers to technical manuals produced by ICAO. The high level ICAO SARPs in Annex 10 Volume III [26] are complemented by the detailed technical specifications in ICAO Doc 9880 and Doc 9705, which in turn refer to international standards and profiles for message handling systems. The ICAO EUR manuals refine and adapt the AMHS specifications for the specific Regional environment.

## 1.5 Document Status

1.5.1 In accordance with Article 4.1b of the interoperability Regulation [1], this EUROCONTROL Specification is proposed for recognition as an EU Community specification within the SES regulatory framework. As such, it will have the status of a voluntary standard, offering a recognised means of compliance with SES regulatory materials and relevant ICAO provisions for ground-ground ATS messaging systems and constituents.

1.5.2 It is intended to be used notably in order to refine and complement the essential requirements laid down in the interoperability Regulation to provide measures aimed at ensuring the interoperability of the EATMN.



- 1.5.3 The EUROCONTROL Regulatory and Advisory Framework (ERAF)<sup>3</sup> has set up the basis for the development of EUROCONTROL Specifications.
- 1.5.4 A EUROCONTROL Specification, after being referenced in the Official Journal of the European Union, can give a formal presumption of conformity with identified essential requirements and regulatory provisions. When an EATMN stakeholder system specification complies with the requirements of such a EUROCONTROL Specification, there is no need to justify separately that the specification defines means of compliance with identified essential requirements and regulatory provisions.
- 1.5.5 It is expected that ANSPs will plan to implement the complete set of requirements specified in this document and its normative Annexes, and obtain the relevant EC declaration.
- 1.5.6 However, it is recognised that during the transition period from AFTN to full ATSMHS capability, intermediate deployment steps will be necessary, as indicated in section 7 below. This EUROCONTROL Specification is structured to facilitate such step-wise implementation:
- During the transition period, interoperability at the Basic ATSMHS level of service can be achieved as specified in Annex A. ANSPs may choose initially to deploy the Basic level of service as an interim step towards full compliance with this EUROCONTROL Specification.
  - As support for the features of the Extended ATSMHS becomes available, including support for binary data, compliance can be assessed against the requirements in Annex B.
  - Deployment and use of the ATN Directory in support of the Extended ATSMHS can be assessed against the requirements in Annex C.
  - It is recognised that the provision of AMHS Security services is not as advanced as other elements of the Extended ATSMHS. For that reason, the specifications in Annex D are considered as advisory.

## 1.6 Applicability

- 1.6.1 The provisions of this EUROCONTROL Specification are applicable to ANSPs in EU Member States. Specifically, the provisions apply to the parts of an ANSP's organisation responsible for providing, directly or by outsourcing, data messaging services to end users both within and between States.
- 1.6.2 The provisions of this EUROCONTROL Specification are indirectly applicable to manufacturers of AMHS End Systems, who may be required to produce an EC declaration of conformity (to the essential requirements).
- 1.6.3 Although targeted to become a Community specification in the EU SES framework, the EUROCONTROL Specification on AMHS would be equally

---

<sup>3</sup> EUROCONTROL Regulatory and Advisory Framework:  
[http://www.eurocontrol.int/enprm/public/standard\\_page/enprm04002.html](http://www.eurocontrol.int/enprm/public/standard_page/enprm04002.html)

applicable to non-EU States in the ICAO EUR Region. It may also voluntarily be applied worldwide.

1.6.4 In terms of the EATMN systems defined in the SES Interoperability Regulation [1], Annex I, this EUROCONTROL Specification specifies interoperability requirements for a "communications system and procedures for ground-to-ground communications," which supports the communications requirements of other EATMN systems.

1.6.5 The basic feature of specifications such as these within the EUROCONTROL Regulatory and Advisory Framework is that they are voluntary standards, which may be adopted by Stakeholders.

1.6.6 In this function such voluntary standards contribute positively to the quest for interoperability as part of the related SES Regulations and Directives.

## **1.7 Conventions**

1.7.1 Only the minimum subset of requirements necessary for the correct and harmonised implementation of the EUROCONTROL Specification is specified. Mandatory items within the EUROCONTROL Specification are clearly separated from non-mandatory items.

1.7.2 Every requirement and recommendation in this specification is preceded by a structured identifier which can be used to reference uniquely the requirement / recommendation from associated documents and traceability tools. Such identifiers have the form:

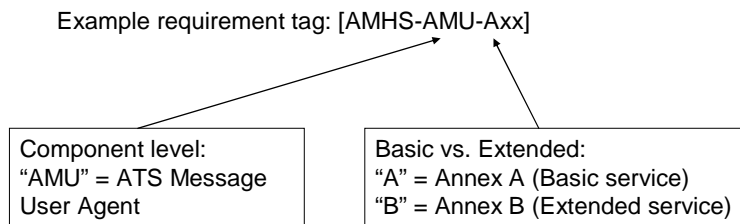
AMHS-[Fn]-[Ann]

where:

[Fn]: is a sequence of characters to identify the operational procedure or category to which the requirement applies, e.g. DIR for general requirements related to Directory functions.

[Ann]: is the Annex identifier followed by a number, unique within a given [Fn];

1.7.3 An example requirement identifier is shown in Figure 2. Note that the structure of requirement identifiers allows differentiation between the Basic ATSMHS and Extended ATSMHS and also identifies the major system components, which can be considered as candidate EATMN constituents.



**Figure 2: Requirement identifier format**

1.7.4 Conventions for denoting requirements in the normative Annexes A, B and C are as follows:

- 'Shall' - indicates a statement of specification, the compliance with which is mandatory to achieve the implementation of the EUROCONTROL Specification. It indicates a requirement which must be satisfied by all systems claiming conformity to the specification. Such requirements are intended to be testable and their implementation auditable.
- 'Should' - indicates a recommendation or best practice, whose use is encouraged, but which may or may not be satisfied by all systems claiming conformity to the specification.
- 'May' – indicates an optional feature.
- 'Will' – is meant in its normal English usage to indicate a forward-looking statement or statement of intent.

## 1.8 Abbreviations and Definitions

### 1.8.1 Abbreviations

The following abbreviations are used throughout this Main Body and associated Annexes:

84IW	1984 Interworking (MHS functional group)
ACP	ICAO Aeronautical Communications Panel
ACSE	Association Control Service Element
ADEXP	EUROCONTROL Standard for ATS Data Exchange Presentation
AF-Address	AFTN-form address
AFS	Aeronautical Fixed Service
AFSG	Aeronautical Fixed Service Group (ICAO EUR Regional group)
AFTN	Aeronautical Fixed Telecommunication Network
AIRAC	Aeronautical Information Regulation And Control
AMC	ATS Messaging Management Centre
AMHS	ATS Message Handling System
AMHxx	Application profile for MHS standards
ANSP	Air Navigation Service Provider
API	Application Programming Interface

EUROCONTROL SPECIFICATION  
on the  
Air Traffic Services Message Handling System (AMHS)

---

ASN.1	Abstract Syntax Notation One
ATM	Air Traffic Management
ATN	Aeronautical Telecommunication Network
ATS	Air Traffic Services
ATSMHS	ATS Message Handling Service
AU	Access Unit
BC	Business Class
CA	Certificate Authority
CAAS	Common AMHS Addressing Scheme
CFMU	Central Flow Management Unit
CIC	Content Integrity Check
CIDIN	Common ICAO Data Interchange Network
CLNP	Connectionless Network Protocol
CNS/ATM	Communications Navigation and Surveillance / Air Traffic Management
COM	Communication
COTS	Commercial-off-the-Shelf
CP	Certificate Policy
CPS	Certificate Practice Statement
CRL	Certificate Revocation List
CSV	Comma Separated Values
CV	Conversion
DAP	Directory Access Protocol
DAP/CSP	Directorate ATM Programmes / Communications Systems and Programmes
DIB	Directory Information Base
DIR	Directory
DISP	Directory Information Shadowing Protocol
DIT	Directory Information Tree
DL	Distribution List
DMD	Directory Management Domain
DMZ	De-militarised Zone
DN	Distinguished (Directory) Name
Doc	ICAO Document
DOP	Directory Operational Binding Protocol
DSA	Directory System Agent
DSP	Directory System Protocol
DUA	Directory User Agent
EANPG	ICAO European Air Navigation Planning Group
EATMN	European Air Traffic Management Network
EC	European Community
ECDSA	Elliptic Curve Digital Signature Algorithm
ECIP	European Convergence and Implementation Plan
ED	EUROCAE Document
EIT	Encoded Information Type
ENPRM	EUROCONTROL Notice of Proposed Rule Making
ER	Exempted Recipients (MHS context)
ER	Essential Requirement (SES context)
ERAF	EUROCONTROL Regulatory and Advisory Framework
ETSI	European Telecommunications Standards Institute
EU	European Union
EUR	ICAO European Region
EUROCAE	The European Organization for Civil Aviation Equipment
FG	Functional Group
FHA	Functional Hazard Assessment

EUROCONTROL SPECIFICATION  
on the  
Air Traffic Services Message Handling System (AMHS)

---

FIPS	Federal Information Processing Standard
FTBP	File Transfer Body Part
HMI	Human-Machine Interface
IA5	International Alphabet Number 5
ICAO	International Civil Aviation Organisation
ICS	Implementation Conformance Statement
Id	Identifier
IEC	International Electro-technical Commission
IETF	Internet Engineering Task Force
IHE	IPM Heading Extension
IP	Internet Protocol
IPM	Interpersonal Message
IPN	Interpersonal Notification
IPS	Internet Protocol Suite
IPsec	Internet Protocol Security (RFC 4301)
IPv4	Internet Protocol version 4 (RFC 791)
IPv6	Internet Protocol version 6 (RFC 2460)
IR	SES Implementing Rule
IRV	International Reference Version
ISO	International Organisation for Standardisation
ISP	International Standardised Profile
ITU-T	International Telecommunication Union – Telecommunications Sector
LD	Latest Delivery
LDAP	Lightweight Directory Access Protocol
LDIF	LDAP Data Interchange Format (RFC 2849)
MD	Management Domain
MF-Address	MHS-form address
MHS	Message Handling System
MM	Military Messaging
MMHS	Military Message Handling System
MOC	Means of Compliance
MS	Message Store
MTA	Message Transfer Agent
MTCU	Message Transfer and Control Unit
MTS	Message Transfer Service
NAT	ICAO North Atlantic Region
NATO	North Atlantic Treaty Organisation
NB	Notified Body
NIST	USA National Institute of Standards and Technology
NOTAM	Notice to Airmen
NRN	Non-Receipt Notification
O/R	Originator / Recipient
OCSP	Online Certificate Status Protocol (RFC 2560)
OHI	Optional Heading Information
OID	Object Identifier
OPA	Operational Performance Assessment
OSA	Operational Safety Assessment
OSD	Operational Services and Environment Definition
OSI	Open Systems Interconnection
OU1	Organisational Unit One (in AMHS address)
P1	MHS Protocol for message transfer
P2	MHS Protocol for interpersonal messaging
P3	MHS Protocol for message submission and retrieval between UA and MTA

EUROCONTROL SPECIFICATION  
on the  
Air Traffic Services Message Handling System (AMHS)

---

P7	MHS Protocol for message indirect submission and retrieval from MS
P772	Military messaging protocol
PAG	PKI Assessment Guidelines
PD	Physical Delivery
PDR	Proposed Defect Report (on ICAO Doc 9705)
PEN(S)	Pan-European Network (Service)
PICS	Protocol Implementation Conformance Statement
PKI	Public Key Infrastructure
PRL	Profile Requirements List
QoS	Quality of Service
RA	Registration Authority
RCP	Required Communication Performance
RDN	Relative Distinguished Name
RED	Redirection
RFC	Request For Comments (IETF)
RN	Receipt Notification
RoC	Return Of Content
ROSE	Remote Operations Service Element
RTCA	Radio Technical Commission for Aeronautics, Inc.
RTSE	Reliable Transfer Service Element
S0	Security Class zero
SARPs	ICAO Standards and Recommended Practices
SDG	Specification Drafting Group
SEC	Security
SES	Single European Sky
SESAR	Single European Sky ATM Research
SHA	Secure Hash Algorithm
SHS	Secure Hash Signature
SNMP	Simple Network Management Protocol (RFC 1157)
SPACE	Study and Planning of AMHS Communications in Europe
SPR	Safety and Performance Requirements Specification
SSA	System Safety Assessment
SSO	System Security Object.
STANAG	NATO Standards Agreement
SV	Sub-Volume of ICAO Doc 9705
TCP/IP	Transmission Control Protocol / Internet Protocol
TP0	ISO Transport Protocol Class 0
TP4	ISO Transport Protocol Class 4
TTP	Trusted Third Party
UA	User Agent
WAN	Wide Area Network
X.400	ITU-T message handling recommendations
X.500	ITU-T Directory recommendations
X.509	ITU-T Recommendation defining public key certificate format
XF-Address	Translated-form address
XMIB	Cross-Domain Management Information Base

## 1.8.2 Definitions

This section defines the terms specific to this document, as well as some common terms which are included for ease of reference. Other definitions may be included by reference to other documents.

EUROCONTROL SPECIFICATION  
on the  
Air Traffic Services Message Handling System (AMHS)

---

AMHS	<p>The set of end systems providing the ATSMHS. In this document, “AMHS” refers only to that part of the global AMHS which is implemented in the EATMN unless otherwise stated, including the interfaces at boundaries with third countries. The AMHS comprises a set of ATN End Systems of type:</p> <ul style="list-style-type: none"> <li>- ATS Message Server, which includes an MTA, optionally one or more MS(s) and, for the support of the Directory Service, a DUA;</li> <li>- ATS Message User Agent which includes a UA and, for the support of the Directory Service, a DUA;</li> <li>- AFTN/AMHS Gateway which includes an MTA, an AU and, for the support of the Directory Service, a DUA.</li> </ul>
AMHS Component	One of the functional objects identified in ICAO Doc 9880 Part IIB [5] which form part of an AMHS End System; i.e. an MTA, UA, MS, AU or DUA.
AMHS End System	An ATN End System participating in the provision of the ATSMHS; either an ATS Message Server, ATS Message User Agent or AFTN/AMHS Gateway.
ANSP (Air Navigation Service Provider)	A body that manages flight traffic on behalf of a company, region or country. It is a provider of air traffic control services.
ATN End System	A computer system that supports one of the ATN applications identified in ICAO Annex 10 Volume III Part I Chapter 3 [26] “Aeronautical Telecommunication Network”.
ATSMHS	<p>The air traffic services message handling service (ATSMHS) application aims at providing generic messaging services over the Aeronautical Telecommunication Network (ATN). Two levels of service are defined within the ATSMHS:</p> <ul style="list-style-type: none"> <li>- The Basic ATSMHS;</li> <li>- The Extended ATSMHS.</li> </ul>
CA (Certificate Authority)	<p>In cryptography, a certificate authority (CA) is an entity which issues digital certificates for use by other parties, containing a public key and the identity of the owner. A CA is an example of a trusted third party (TTP) which is characteristic of many public key infrastructure (PKI) schemes. The CA also attests that the public key contained in the certificate belongs to the person, organisation, server or other entity noted in the certificate. Optionally the certificate authority may create the users' keys.</p> <p>(As noted in ICAO Doc 9705 §8.3.1.2.2, the term “Certificate Authority” is used rather than “Certification Authority” due to the common use of the latter term in the aviation community for aircraft certification, etc).</p>
(Public Key) Certificate	A data structure containing a public key and some other information, which is digitally signed with the private key of the CA which issued it ( <i>IETF Definition</i> ). The end entity, i.e. the user of the certificate, can be an end-user, an application or a device. A certificate can be associated with an end entity or with a CA.
Constituents	Tangible objects such as hardware and intangible objects such as software upon which the interoperability of the EATMN depends ( <i>SES framework Regulation 549/2004 [23]</i> ). Constituents would normally be identified in interoperability implementing rules (IR) in accordance with Article 3 of the SES Interoperability Regulation 552/2004 [1], but in this case there is no IR.

EUROCONTROL SPECIFICATION  
on the  
Air Traffic Services Message Handling System (AMHS)

---

CP (Certificate Policy)	A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. <i>(ITU-T X.509 [35])</i>
CPS (Certificate Practice Statement)	Defines how a specific CA meets the technical, organisational and procedural requirements identified in a certificate policy.
EATMN	The collection of systems listed in Annex I to Regulation (EC) No 552/2004 (the interoperability Regulation) enabling air navigation services in the Community to be provided, including the interfaces at boundaries with third countries" <i>(SES framework Regulation 549/2004 [23])</i> .
EATMN systems	The EATMN systems within the scope of this EUROCONTROL Specification are "Communication systems and procedures for ground-to-ground ... communications" <i>(Regulation 552/2004, Annex I)</i> and other systems which interface with them.
End System	A system that contains the seven layers defined in the basic reference model for open systems interconnection including one or more end user application processes.
End-to-end	Pertaining or relating to an entire communication path, typically from (1) the interface between the information source and the communication system at the transmitting end to (2) the interface between the communication system and the information user or processor or application at the receiving end <i>[Annex 10 Volume III Part 1 [26]]</i> .  In the context of this EUROCONTROL Specification, "end-to-end" is taken to mean the path between a message originator and the addressee(s) of that message.
Interoperability	'Interoperability' means a set of functional, technical and operational properties required of the systems and constituents of the EATMN and of the procedures for its operation, in order to enable its safe, seamless and efficient operation. Interoperability is achieved by making the systems and constituents compliant with the essential requirements. <i>[SES framework Regulation 549/2004 [23]]</i>
Interoperability Target	An interoperability target is a description of specific operational, functional and/or technical elements within the EATMN used to support the identification of regulatory and specification provisions. Used within a EUROCONTROL Specification, it provides a high level operational and services environment description that supports understanding of what is to be achieved.
Notified Body (NB)	<i>(Refer to Article 8 of the interoperability Regulation [1])</i> . A body which carries out the tasks pertaining to the conformity assessment procedures referred to in the applicable EC New Approach directives when a third party is required. With the "Recognised Third Party Organisations" and "User Inspectorates", "Notified Bodies" is a type of body involved with Conformity Assessment. For example, "EC" verification is the procedure whereby a notified body checks and certifies that a subsystem: <ul style="list-style-type: none"> <li>• complies with the Directive</li> <li>• complies with the other regulations deriving from the Treaty, and may be put into operation.</li> </ul>
RA (Registration Authority)	An authority which receives certificate requests and which verifies the acceptance of the request by verification of the requester and sends the request to the CA.



Security policy	A set of objectives, rules of behaviour for users and administrators, and requirements for system configuration and management that collectively are designed to safeguard systems and communication resources concerned with the provision of communication services against acts of unlawful interference.
TTP (Trusted Third Party)	An entity trusted by other entities with respect to security-related services and activities. As this party is trusted, it can act as a CA. The TTP will be an organisation, licensed or accredited by a regulatory authority.

## 1.9 Interoperability Target

1.9.1 In a generic specification such as this it is impossible to foresee all possible messaging configurations. The actual environment will have to be elaborated as part of the detailed specification for each individual implementation.

1.9.2 The functional environment specification includes:

- Required gateway functionality;
- Messaging systems that are to be interconnected;
- Available communications and network infrastructure.

1.9.3 A messaging system in terms of this EUROCONTROL Specification may be required to interwork with:

- ATS Message Servers within a State or in other States, implementing the ATSMHS over ATN/IPS transport services;
- ATS Message User Agents, for the local submission and delivery of messages by "direct" ATSMHS users;
- AFTN/AMHS Gateways, for the transition of AMHS messages into the AFTN, and vice-versa;
- National and/or multi-national directory services.

1.9.4 Possible interworking with other message handling systems is a local matter, outside the scope of this EUROCONTROL Specification.

1.9.5 To ensure seamless operation, there are interoperability requirements at a number of distinct levels:

- Geographical

The ATSMHS is applicable within and between countries. The ATS Message Server topology needs to be optimised for efficient routing in this context.

- Procedural

The ATSMHS must be used in a consistent way to ensure a seamless service. Procedures must be specified for day-to-day configuration and

operation of the message handling service, as well as for orderly transition from legacy systems.

- Human-machine interface (HMI)

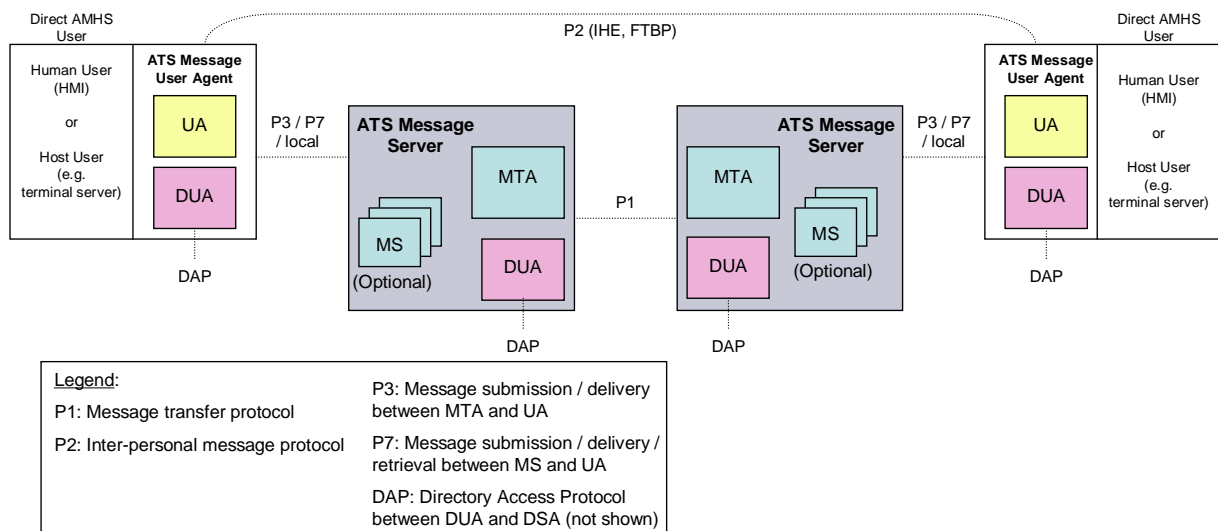
For direct AMHS users in the human user subgroup, the HMI must offer the required input capabilities and display the required information. However, human factors / ergonomics are out of scope of this EUROCONTROL Specification.

- Communication protocols

Ground end systems must interwork at the technical level. End systems must interwork with logically adjacent end systems (e.g. an ATS Message User Agent must interwork with an ATS Message Server for message submission and delivery) as well as with peer end systems (i.e. interworking between AMHS users, both direct and indirect). The end system includes:

- Application entities (e.g. MTA, MS, UA, DUA, DSA)
- Upper Layers (above transport layer)
- Lower Layers (transport layer and below)

1.9.6 Figure 3 illustrates the interoperability target for AMHS.



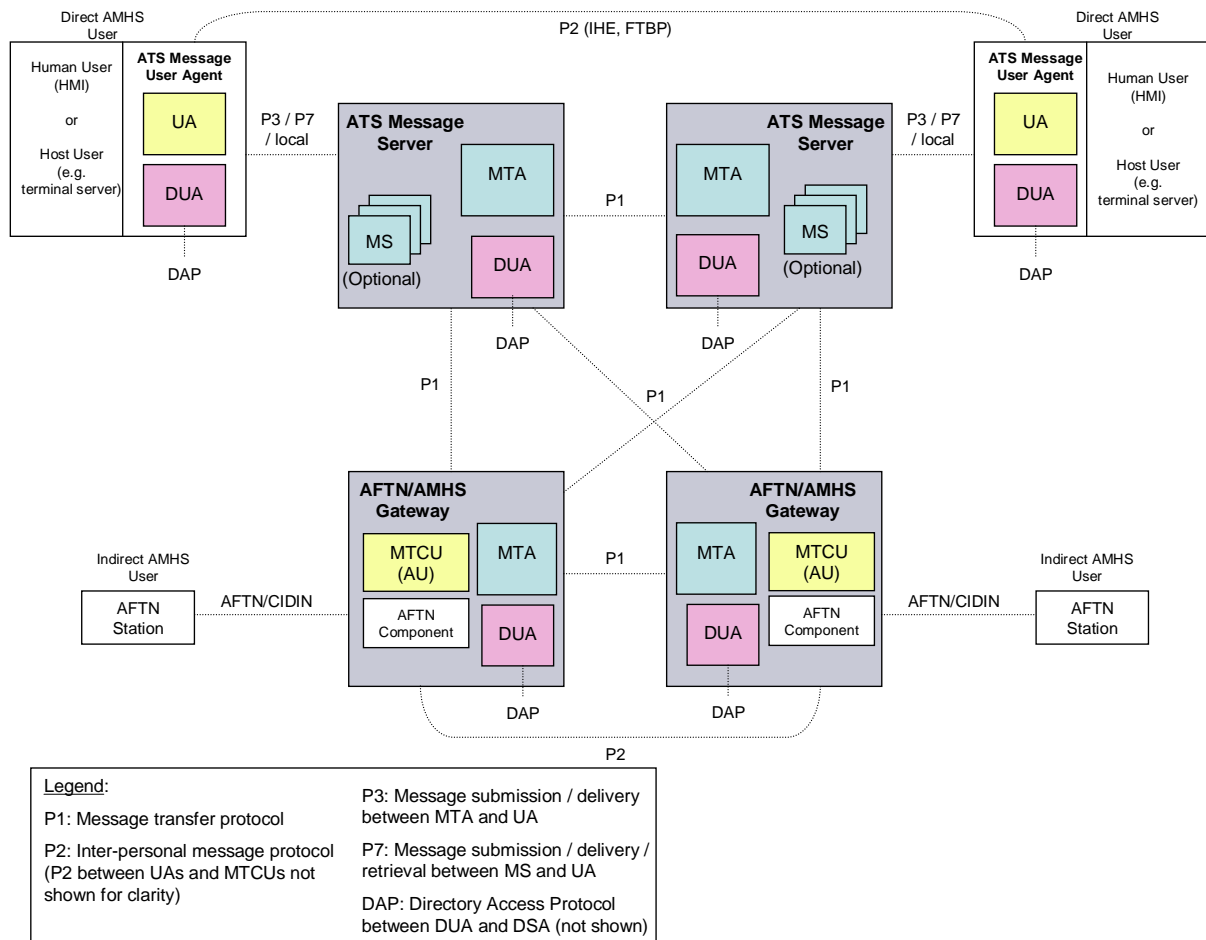
**Figure 3: AMHS Interoperability Target**

1.9.7

The ATS Message User Agent is a logical component that may or may not be physically identifiable in an implementation. It may be either logically co-located or remote from the ATS Message Server with which it is associated. When logically remote from the ATS Message Server, it will use the P7 protocol if using a Message Store (MS), or the P3 protocol if communicating directly with the Message Transfer Agent (MTA). The MS is an optional component of the ATS Message Server.

- 1.9.8 If end-to-end message security services are implemented, the user agent (UA) components would need additional functionality for generating and verifying the content integrity check and digital signature, and there would need to be additional infrastructure to support the management of public key certificates. Note that there are also security measures applied to ATS Message Servers and DSAs, as well as link level security.
- 1.9.9 The directory function (DIR), accessed via a Directory User Agent (DUA) which communicates with a Directory System Agent (DSA), provides an enhanced level of service, supporting functions such as address lookup and enabling a message originator to determine the capability of an intended recipient (direct AMHS user) before initiating the message exchange. The DUA is a mandatory component of the ATS Message Server and ATS Message User Agent when these end systems support the Extended ATSMHS. The DUA enables access to the ATN Directory by means of the Directory Access Protocol (DAP). Note that within a local system, other access protocols such as LDAP may be considered.
- 1.9.10 During the transition phase, which may take a number of years, legacy AFTN systems and terminals will need to be supported, both within States and between States. A State which has an operational AMHS may still support legacy AFTN users within that State (indirect AMHS users), and will also need to interwork with States that do not have operational AMHS deployments.
- 1.9.11 The goal is for interoperability between end users. Clearly, the degree of interoperability possible will depend upon the capability of the end user's system. For example, an AFTN terminal would not be expected to interoperate with an ATS Message User Agent for the exchange of binary encoded weather maps. However, basic interoperability at the level of ATS message exchange (textual rendition of flight plan, etc. messages) would be supported, and would be achieved through the use of an AFTN/AMHS gateway.

EUROCONTROL SPECIFICATION  
on the  
Air Traffic Services Message Handling System (AMHS)

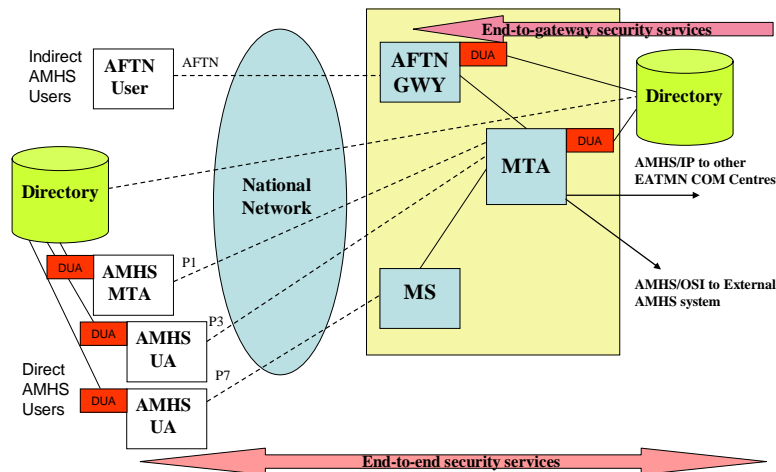


**Figure 4: AMHS Interoperability Target (transitional phase)**

- 1.9.12 Figure 4 illustrates the elements which are needed for transition, and represents the initial Interoperability Target.
- 1.9.13 The DUA is a mandatory component of the AFTN/AMHS Gateway when the Extended ATSMHS is supported. If an AFTN/AMHS Gateway additionally supports message security services, the access unit (AU) components would need additional functionality for verifying the content integrity check and digital signature.
- 1.9.14 At a future date, when the transition from AFTN/CIDIN is complete, and no legacy AFTN stations remain, the AFTN/AMHS Gateways will no longer be required. The ultimate interoperability target for AMHS is for all end users to become Direct AMHS users.
- 1.9.15 Figure 5 illustrates the initial interoperability target from the perspective of a European international COM Centre. It shows:
- An ATS Message Server, comprising an X.400 message transfer agent (MTA) and optionally one or several message stores (MS), and a Directory

User Agent (DUA). The ATS Message Server uses the P1 protocol over TCP/IP to communicate with other ATS Message Servers and with AFTN/AMHS Gateways in the EATMN.

- b) The MTA may optionally use “dual stack” ATN/OSI (or other bilaterally agreed solution) and ATN/IPS lower layer protocols to communicate via P1 with ATS Message Servers and AFTN/AMHS Gateways outside the EATMN.
- c) An AFTN/AMHS Gateway, which includes an AFTN component, an ATN component (MTA), a Message Transfer and Control Unit (MTCU), a Control Position and a DUA. The MTA may in actuality be the same MTA in a) above. The MTCU is an MHS access unit.
- d) A Directory service, comprising one or more interconnected or free-standing DSAs.
- e) Access to the COM Centre by Indirect AMHS user using the AFTN/AMHS gateway.
- f) Access to the COM Centre by Direct AMHS user, comprising an ATS Message User Agent using P3 and/or P7 protocols and a DUA.
- g) Interconnection of the COM Centre with another ATS Message Server, which is part of the State’s internal messaging system using P1 protocol.
- h) End-to-end message security services for direct AMHS users, which may be bilaterally agreed. (For indirect AMHS recipients, the message security may be established between a sending AMHS direct user and AFTN/AMHS Gateway).
- i) An abstract “National Network,” which may be composed of several networks, leased lines, dial-up connections, etc. providing connectivity between end systems within a State. In some cases an ATS Message User Agent may be connected using other networks instead of, or additionally to, the national network.



**Figure 5: COM Centre perspective**

- 1.9.16 The functional model and architectures depicted in this section provide an abstract, logical view of AMHS functional components. UA and MS functionality may be implemented, for example, by means of an AMHS terminal server providing centralised UA/MS functionality, and supporting AMHS protocols and message formats. The dialogue between the user workstation itself and the terminal server is then a matter local to the State and considered ANSP.
- 1.9.17 In the full scope of European ATS message handling, there could also be one or more gateway(s) to/from local non-AMHS message handling systems, but this is outside the scope of this EUROCONTROL Specification.
- 1.9.18 To enable the interoperability target to be reached, this EUROCONTROL Specification defines means of compliance largely by reference to external standards and documents maintained by ICAO and EUROCAE. In turn, these documents also reference many ISO/IEC standards and ITU-T Recommendations.
- 1.9.19 This EUROCONTROL Specification references such change control mechanisms as necessary (e.g. ICAO Amendment Proposals, EUROCAE Improvement Suggestion Forms) that are used by the bodies responsible for maintaining the referenced standards and documents.

## 1.10 Responsible Unit

- 1.10.1 This EUROCONTROL Specification has been developed and is maintained by the Communication (CO) Unit of the CNS section within the Centre of Expertise (CoE) division of the Directorate Cooperative Network Design (CND) of the European Organisation for the Safety of Air Navigation (EUROCONTROL).

## **2. AMHS INTEROPERABILITY – BASIC ATSMHS**

### **2.1 General**

2.1.1 This chapter contains guidance and explanatory material for the AMHS Interoperability requirements in Annex A, which apply to the Basic ATSMHS level of service as defined in ICAO Doc 9880 Part IIB [5].

### **2.2 Standards Baseline**

2.2.1 The standards baseline in Annex A defines the standards which through reference constitute part of the EUROCONTROL Specification.

2.2.2 The approach is to reference ICAO material where available, noting deviations where required and specifying additional functionality where necessary.

2.2.3 ICAO Annex 10 Volume III [26] refers to the detailed technical specifications for the ATSMHS in ICAO Doc 9880 Part IIB [5]. These provisions in turn make reference to International Standardised Profiles (ISPs) published by the International Organisation for Standardisation (ISO).

2.2.4 In the MHS base standards (ISO/IEC 10021 and ITU-T X.400 [18]), a subset of the OSI Upper Layer protocols (ROSE, RTSE, ACSE, Presentation and Session layers) is used to support communications between the MHS components (MTA, UA, AU and MS). The use of OSI upper layers is specified in a common ISP applicable to each MHS component.

2.2.5 The referenced ISPs also include profiles for common messaging and for inter-personal messaging (IPM).

2.2.6 However, there remain some options and implementation choices in the AMHS technical specifications in ICAO Doc 9880 Part IIB [5]. These include support of the Extended and/or Basic ATSMHS, support for different body part types, message size constraints, etc.

2.2.7 The responsible group (AFSG) within the ICAO European Region (EUR) has produced the EUR AMHS Manual (ICAO EUR Doc 020 [8]), which provides general guidance and detailed information on requirements concerning AMHS implementation in the ICAO EUR Region.

2.2.8 The ICAO European Regional office has also published the ATS Messaging Management Manual (ICAO EUR Doc 021 [9]), which describes the framework in which the services of the ATS Messaging Management Centre (AMC) are provided, and also describes the procedure for the introduction of a new AMHS COM Centre in the international EUR/NAT AMHS network.

## 2.3 Network Support

- 2.3.1 This section describes interoperability between the AMHS components (MTA, UA, etc.) and the supporting network infrastructure. In general, there will be network level security features such as firewalls to control access to the infrastructure. Security protocols such as IPsec can be used to ensure that only named servers can connect to one another. However, these are not specific to the messaging system and are not described further.
- 2.3.2 As specified in ICAO Doc 9880 Part IIB [5], an AMHS End System can make use of the connection mode transport service provided by either or both of the ATN/OSI or the ATN/IPS. In the former case, it operates over the ATN internet communications service, based on a TP4/CLNP protocol stack, while in the latter case it operates over a TCP/IP protocol stack.
- 2.3.3 Implementations by ANSPs in Europe will make use of a ground-ground network infrastructure based on TCP/IP, as specified in ICAO EUR Doc 020 [8], section 3.5. This is consistent with the ATN/IPS as defined in ICAO Doc 9896 [22], and with the option to use the ATN IPS transport service as defined in ICAO Doc 9880 Part IIB [5], section 3.2.2.2.3.
- 2.3.4 An underlying network infrastructure that can provide physical connectivity between international ATS Message Servers needs to be implemented as a Common Facility, in a timeframe compatible with the AMHS deployment plan. It is foreseen that this will be provided by the Pan-European IP network (PEN). Bilateral or multilateral connectivity arrangements can accommodate initial AMHS operations, until such a common facility becomes available.
- 2.3.5 TCP/IP is specified for interconnections between MTAs of different ANSP international COM Centres within Europe. The same lower layer profile may also be used within an ANSP's local systems – e.g. to support P1, P3 and P7 transfer and access protocols.
- 2.3.6 Additional protocol stacks may be required in other situations (e.g. the ATN/OSI profile may be additionally required in EATMN boundary systems, and other profiles may need to be used between the MTAs operating within an ANSP's Management Domain).

## 2.4 Safety and Performance Requirements

- 2.4.1 In terms of the SES Interoperability Regulation [1]:
- "Communication systems shall be designed, built, maintained and operated using the appropriate and validated procedures, in such a way as to achieve the required performances ... for a specific application, in particular in terms of communication processing time, integrity, availability and continuity of function."*
- 2.4.2 Detailed safety and performance requirements (SPR) are specific to the applications using the ATSMHS. Safety and performance requirements for a



particular operational environment are typically enumerated in a SPR specification, as defined in ED-78A [11], and are the products of operational safety assessment (OSA) and operational performance assessment (OPA) processes.

- 2.4.3 Safety requirements are shared risk mitigation strategies that aim at satisfying safety objectives. Safety objectives apply, for example, to the probability of undetected message loss or corruption. The severity of the hazard depends upon the nature of the message, i.e. upon the user application, and is assessed during the OSA process for that application.
- 2.4.4 Within the Extended ATSMHS, security services can help to protect against safety hazards such as accidental or deliberate message corruption and can provide protection against undetected misdelivery. Note that additional functions are necessary to protect against other threats such as messages containing computer viruses.
- 2.4.5 The OSA and OPA are dependent upon the specific operational services and environment definition (OSD). The OSA determines, validates, and allocates requirements to ensure that the CNS/ATM system, as described in the OSD, is acceptably safe. The OPA derives and/or validates required communication performance (RCP) type.
- 2.4.6 For the operational hazard assessment (part of the OSA), services are examined to identify and classify hazards that could adversely affect those services. For AMHS, the hazard depends upon the safety-criticality of the message content. High-level hazards (e.g. probability of message loss or corruption) can be identified, but not quantified for the AMHS in isolation.
- 2.4.7 Implementers will have to show for approval that the relevant SPR standards are satisfied per ED-78A [11] Section 5 (Development and Qualification of a System Element) and Section 6 (Entry into Service).

## **2.5 Message Transfer Service Interoperability**

- 2.5.1 This section is concerned with MTA-to-MTA interoperability requirements.
- 2.5.2 The Message Transfer Service (MTS) is provided by MTAs communicating via the message transfer protocol P1. The profile requirements for MTAs in the EATMN will be as specified in ICAO EUR Doc 020 [8], Appendix B section 4.5.
- 2.5.3 There is a clear distinction in the design of the European AMHS between national and international communications. Each European State/ANSP implementing an AMHS management domain may decide to decouple the international AMHS from its national messaging network by the setting up of one or more international ATS Message Servers (together with an AFTN/AMHS Gateway if necessary for transition purposes) forming the interconnection point between both environments.

2.5.4 A backup ATS Message Server may be specified to take over from an international ATS Message Server if the primary system becomes unavailable.

2.5.5 An important consideration is the topology to be adopted for ATS Message Servers if more than one is to be deployed for the State AMHS service. Nationally, the AMHS architecture of ATS Message Servers can be centralised or distributed. This is discussed in section 3.3 of ICAO EUR Doc 020 [8].

## **2.6 End to End Interoperability of Direct AMHS Users**

2.6.1 This section is concerned with UA-to-UA interoperability requirements.

2.6.2 A direct AMHS user is a human or automated system that uses an ATS Message User Agent for message submission and delivery.

2.6.3 The ATSMHS is based on the standards for the interpersonal messaging protocol (P2), i.e. ISO/IEC 10021-7 | ITU-T Recommendation X.420 [18], using message content type 22.

2.6.4 Users of the Basic ATSMHS are able to send and receive simple text messages using a single ia5-text body part containing a structured ATS Message Header.

## **2.7 Interoperability between AFTN and AMHS**

2.7.1 This section is concerned with AFTN/AMHS Gateway requirements.

2.7.2 During the transition phase from AFTN/CIDIN to the AMHS, the interoperability between AFTN and AMHS is achieved by the use of AFTN/AMHS gateways.

2.7.3 Interconnection between the AFTN/CIDIN and the AMHS in Europe will be by means of AFTN/AMHS Gateways directly interfacing with the AFTN application supported by European international AFTN/CIDIN COM Centres.

2.7.4 Technical provisions for the AFTN/AMHS gateway are specified in ICAO Doc. 9880 Part IIB [5], section 4.

## **2.8 Ground Recording of Messages**

2.8.1 Annex A elaborates on the information required to be recorded by AMHS End Systems, in accordance with ICAO recording requirements. These are minimum requirements for recording the message exchanges for audit and incident investigation purposes.

## **2.9 Naming and Addressing**

- 2.9.1 Annex A includes requirements for specifying, maintaining and disseminating unambiguous name and address information required for safe and efficient operation of the communications system.
- 2.9.2 ICAO Doc 9880 Part IIB [5] section 2.5.1.4 requires each AMHS management domain to implement an AMHS addressing scheme policy. The management domain may implement either a MHS-form (MF) addressing scheme, or a locally defined addressing scheme, or a combination of both. Two alternative MF-addressing schemes are defined: the Common AMHS Addressing Scheme (CAAS) and the Translated-form (XF) addressing scheme.
- 2.9.3 Adoption of a single EATMN-wide addressing scheme would simplify address management and hence aid seamless operations. Therefore the CAAS is recommended for the EATMN. This is consistent with ICAO Doc 9880 Part IIB, section 2.5.1.4.1.5 and with ICAO EUR Doc 020 [8], section 3.2.5.1.
- 2.9.4 However, for interoperability purposes, all components of Basic and Extended ATSMHS systems must support all of the AMHS address formats identified in ICAO Doc 9880, including XF-addresses. This does not require any form of address translation by an ATS User Agent or an ATS Message Server.

## **2.10 Operational Procedures**

- 2.10.1 Operational procedures for implementing and managing international AMHS are specified by the Aeronautical Fixed Services Group (AFSG) under the auspices of the ICAO European Air Navigation Planning Group (EANPG). Such procedures are documented in ICAO EUR Doc 020 [8], ICAO EUR Doc 021 [9] and Part I of the Routing Directory for COM Centres in the EUR/NAT Regions [27].
- 2.10.2 These procedures, which are applicable for ICAO Contracting States in the EUR Region, are equally applicable to all EATMN countries.

## **2.11 Interoperability with Military Message Handling Systems**

- 2.11.1 It is a requirement of the interoperability Regulation ([1], Annex II) that the EATMN, its systems and constituents support the progressive implementation of civil/military coordination by supporting the timely sharing of correct and consistent information between civil and military parties.
- 2.11.2 Options for military interconnection with AMHS may vary from merely retaining AFTN remote tails, accessing AMHS via gateways, to a certain level of interconnection with military networks including the X.400 based Military Message Handling System (MMHS). The latter solution might raise significant challenges in terms of security and directory services. Discussions at the EUROCONTROL Civil-Military CNS Focus Group indicated that the likely option for initial military access to AMHS is to get connected to ANSP systems

via local AFTN/AMHS gateways or to replace AFTN terminals with ATS Message User Agents (not covered in the present Specification).

- 2.11.3 The EUROCONTROL Civil-Military CNS/ATM Interoperability Roadmap [45], section 5.4.1, Ground networks interoperability, notes:

*"In the area of aeronautical messaging, both the NATO Military Message Handling System (MMHS) and the ICAO AMHS are based on the ISO X.400 standard. Also in this area, security aspects will probably severely constrain any direct interconnection of systems.*

*"AMHS will replace AFTN and CIDIN networks with effect from early 2009 approximately, but will not migrate to operation over PENS until later. Since many military units today rely on AFTN terminals to transfer aeronautical data such as flight plans, NOTAMS, meteorological data, etc., military access to AMHS will remain a civil-military interoperability requirement, probably through local agreements with civil ANSPs."*

- 2.11.4 Note that the MMHS specifications referred to above include STANAG 4406 [43], which defines an X.400 based MHS with extensions for military use, including a possible interface to Civilian MHS via a trusted gateway. The MMHS Elements of Service and protocol are defined as a Military Messaging (MM) content type, identified as the P772 protocol. Several of the Business Class attributes as defined for the Extended ATSMHS (e.g. precedence, originators-reference) can translate easily to P772 equivalents.

- 2.11.5 AMHS connectivity will be an important step towards the network centric architecture System Wide Information Management (SWIM), to be implemented in the sequence of SESAR Target Concept which requires all ATM actors, including military ATC and Air Defence, to be able to exchange information in a distributed and fully automated way.

- 2.11.6 Consequently, medium and longer term civil-military interoperability solutions are likely to include higher levels of connectivity and exchange of aeronautical messaging services including compatible security levels.

## **2.12 Interoperability with Systems External to EATMN**

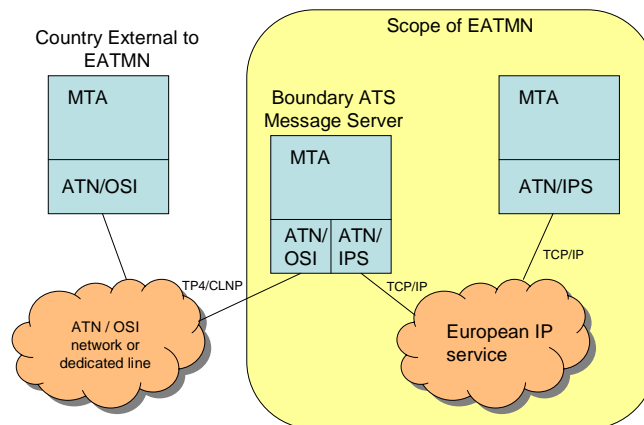
- 2.12.1 Within the EATMN, AMHS communication will be based on ATN/IPS lower layers. Elsewhere in the world, it is possible that AMHS communication could be based on ATN/OSI lower layers. ICAO Annex 10 Volume III [26] requires that regional air navigation agreements will specify the area in which the communication standards for the ATN/OSI or the ATN/IPS are applicable.

- 2.12.2 The decoupling that exists in an AMHS End System between upper layers and lower layers (transport and network services) allows an ATS Message Server to communicate using different lower layers with different adjacent MTAs. Such lower layer stacks can include ATN/OSI and ATN/IPS protocol stacks.

- 2.12.3 The ability to implement AMHS end systems with multiple lower layer stacks may be used if needed to ensure global interoperability at the application

layer. In this model, one ATS Message Server could be nominated as the boundary system for interfacing the EATMN AMHS to the AMHS in third countries.

- 2.12.4 In such a case, the requirements applicable to AMHS End Systems within the EATMN may not be applicable to those system elements responsible for interfacing with external systems, e.g. in terms of performance or protocol support.
- 2.12.5 Provisions for AMHS interworking at boundaries with countries external to the EATMN will normally be concentrated in Boundary ATS Message Servers. If the external systems support only ATN/OSI lower layer protocols, the implementation of dual stacks as illustrated in Figure 6 can be proposed as the interworking solution. Other solutions may also be possible, but are outside the scope of this EUROCONTROL Specification.



**Figure 6: Dual communications stack at Regional boundary**

- 2.12.6 The European AMHS will make use of an ISO TP0 transport service implemented over a TCP/IP stack. If needed, boundary ATS Message Servers in selected boundary COM centres will implement dual stack systems to allow interconnection with ATN/OSI AMHS systems external to the EATMN.
- 2.12.7 It is envisaged that such boundary ATS Message Servers will be implemented as a Common Facility for the benefit of the whole EATMN, to provide AMHS connectivity towards other countries.

### **3. EXTENDED ATSMHS**

#### **3.1 General**

3.1.1 This section contains explanatory material for the requirements in Annex B concerning the Extended ATSMHS.

3.1.2 The Extended ATSMHS is an enabler for ATS operational improvements. It will provide significant operational benefits, improvement of ATS capacity and performance.

3.1.3 The requirements for Extended ATSMHS are in addition to those for Basic ATSMHS.

#### **3.2 Standards Baseline**

3.2.1 The standards baseline in Annex B defines the standards which through reference constitute part of the EUROCONTROL Specification concerned with the Extended ATSMHS.

#### **3.3 Extended ATSMHS Functionality**

3.3.1 All AMHS End Systems supporting the Extended ATSMHS must conform to the relevant requirements of the Basic ATSMHS.

3.3.2 In addition, implementations which support the Extended ATSMHS include functionality which can conveniently be described in terms of the following functional groups:

- a) Use of File Transfer Body Parts (FTBP). This functional group enables the transfer of binary data between direct AMHS users. When binary files can be transferred it is important to include virus protection in the architecture, associated with the ATS Message Server and/or ATS Message User Agent; however this is out of scope of this EUROCONTROL Specification.
- b) Use of IPM Heading Extensions (IHE). This functional group uses standard message fields instead of the AMHS-specific ATS Message Header which is required in the Basic ATSMHS.
- c) AMHS Security (SEC). This functional group enables support of the AMHS security policy, providing message origin authentication and content integrity assurance between direct AMHS users.

- d) Use of Directory (DIR). This functional group enables support of the ATN Directory through the use of a DUA included in the AMHS End System.

3.3.3 An implementation of an ATS Message User Agent or of an ATS Message Server claiming full conformance to ICAO Doc 9880 Part IIB [5] for the Extended ATSMHS is required to support all of these functional groups.

3.3.4 ICAO Doc 9880 Part IIB [5] also allows an implementation of an ATS Message User Agent or of an ATS Message Server to claim conformance for a subset of the Extended ATSMHS, in accordance with one of the valid configurations listed in Table 1.

**Table 1: Definition of ATSMHS subsets**

<b>Configuration Reference</b>	<b>Functional Group Combination</b>
I.	Basic
II.	Basic + FTBP
III.	Basic + IHE
IV.	Basic + DIR
V.	Basic + DIR + FTBP
VI.	Basic + DIR + IHE
VII.	Basic + DIR + SEC
VIII.	Basic + IHE + DIR + SEC
IX.	Basic + IHE + DIR + FTBP
X.	Basic + IHE + DIR + FTBP + SEC

3.3.5 If different AMHS End Systems in the EATMN were to support different combinations of functional groups this would be detrimental to full functional interoperability and seamless operations (although interoperability would be possible at least at the Basic ATSMHS level).

3.3.6 Conformance to this EUROCONTROL Specification for the Extended ATSMHS requires implementation of configuration IX (Basic + IHE + DIR + FTBP functional groups) only.

3.3.7 Note that the future migration to configuration X (addition of SEC) may be foreseen, but is not currently required for compliance with this EUROCONTROL Specification.

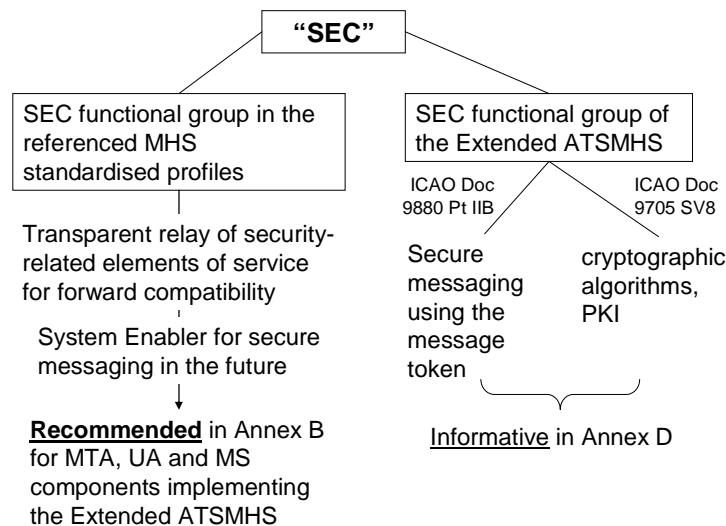
3.3.8 For the AFTN/AMHS Gateway, ICAO Doc 9880 Part IIB does not specify any distinct functional groups; an implementation may or may not support the Extended ATSMHS as a whole. In practice, FTBP is not relevant for an AFTN/AMHS Gateway; if an AMHS message containing an FTBP body part were received it would unconditionally be rejected by the gateway according to ICAO Doc 9880 Part IIB, paragraph 4.5.2.1.4.b). SEC would be applicable in the AMHS-to-AFTN direction. IHE and DIR would be supported by an AFTN/AMHS Gateway that supports the Extended ATSMHS.

3.3.9 For maximum flexibility and forward compatibility, a minimum level of support of the SEC functional group of the P1 profile is recommended in Annex B for the ATS Message Server and AFTN/AMHS Gateway. The minimum support

includes security class S0, as defined in ISO ISP 10611-1 Annex C. Security class S0 is confined to security functionality operating between MTS-users on an end-to-end basis in order to permit transfer across an MTS which may be untrusted. It is designed to minimise the required functionality in the MTS to support the submission of elements associated with these services.

3.3.10 This does not imply that the AMHS user is required to support secure messaging, merely that the MTA supports the required envelope extensions as an enabler for future AMHS user functionality.

3.3.11 It is important to note the distinction between the AMHS functional group SEC and the SEC functional group used in the ISPs. This is illustrated in Figure 7.



**Figure 7: SEC FG in ISPs vs. Extended ATSMHS**

### 3.4 End to End Interoperability of Direct AMHS Users

3.4.1 Users of the Extended ATSMHS have access to advanced features that are not available to users of the Basic ATSMHS. These include binary data transfer using file transfer body part and, if the SEC functional group is implemented, message security features. The profile requirements for UAs in the EATMN are as specified in ICAO EUR Doc 020 [8], Appendix B Annex A (IPM content) and Annex P (message token generation and reception).

3.4.2 Interoperability issues may arise when a user supporting the Extended ATSMHS wishes to communicate with a user supporting the Basic ATSMHS. In such cases, interoperability will only be possible at the Basic ATSMHS level of service.



3.4.3 For example, if a direct user wishes to send a file transfer body part, this will only be meaningful if all of the addressed recipients can process such body part types correctly, i.e. they support the FTBP Functional Group of the Extended ATSMHS. For the sake of robustness, even an ATS Message User Agent supporting only the Basic level of service is expected to be able to receive a message containing unsupported body parts without aborting or malfunctioning.

### **3.5 Naming and Addressing**

3.5.1 In the Extended ATSMHS, the O/R name of an AMHS user is required to comprise both the MF-address (O/R address) and the directory name (distinguished name form) of the AMHS user (see ICAO Doc 9880 Part IIB [5] section 2.5.1.1.2).

3.5.2 This implies conveyance of both MF-address and directory name in the message envelope and IPM heading. In practice, a UA, MTA, or Gateway receiving a message has no use for the received directory names, as it never needs to look anything up in the directory (except possibly a user's certificate, if secure messaging is implemented). Theoretically, support for IPM Use of Directory requires a UA to be able to display the directory component in a received O/R Name (ISO ISP 12062-1 A.2.3).

3.5.3 For maximum interoperability and efficiency, it is recommended that, in addition to the MF-address, a directory name is registered for all direct users, but that Extended AMHS systems do not include the directory name element of O/R Names on message submission.

## **4. USE OF DIRECTORY**

### **4.1 General**

4.1.1 This section contains explanatory material for the requirements in Annex C for the use of Directory by AMHS.

4.1.2 Topics addressed include:

- Directory Architecture in the EATMN (section 4.2);
- Directory System Protocols (DSP, DISP) (section 4.3);
- Directory access (section 4.4);
- Directory Schema (section 4.5);
- Versioning and data life cycle (section 4.6).
- Directory support of PKI (see section 4.7);

4.1.3 In the Basic ATSMHS, the equivalent of a "directory" function may be realised as a simple look-up table of addresses. In the Extended ATSMHS, the directory may be a centralised or fully distributed database, including support for replication, chaining, etc.

4.1.4 ICAO EUR Doc 020 [8] specifies, in Appendix B Annex K (which has Informative status), directory information, in the form of Object Classes and Attribute Types that are useful to support Directory Name resolution and the mapping of AFTN addresses to and from AMHS addresses.

4.1.5 ICAO Doc 9880 Part IVA [7] specifies the ATN Directory service. In particular, a set of ATN Object Classes and Attribute Types are specified for use with systems supporting the Extended ATSMHS.

4.1.6 An ANSP's system specification would need to include requirements for (a) the directory information base, (b) the directory access method and (c) the directory system protocols to be supported.

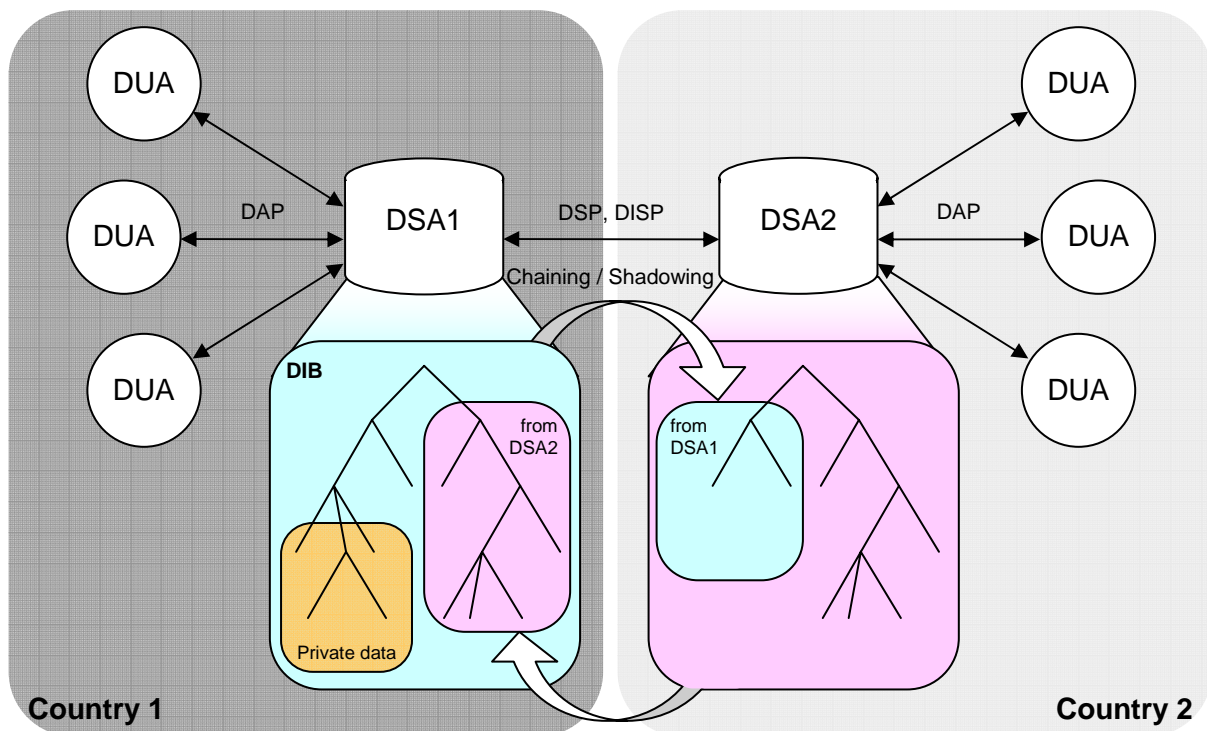
4.1.7 A central Directory Service, implemented as a Common Facility for the benefit of the whole European area, would facilitate AMHS address publication and thus aid address conversion.

### **4.2 Directory Architecture**

4.2.1 This section describes a directory architecture for ANSPs in Europe and details requirements to be met by the Directory System Agents (DSAs) and

Directory User Agents (DUAs), in order to guarantee interoperability and data sharing.

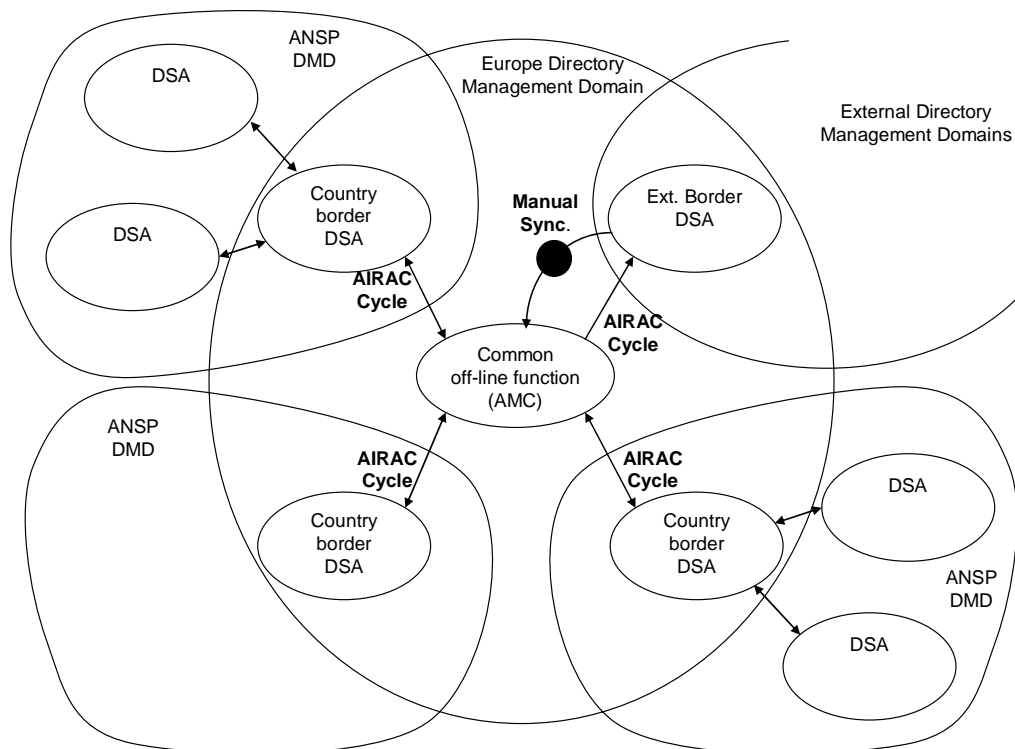
- 4.2.2 The general Directory Service (DIR) allows users to obtain directory information about other users, applications and services participating in the network. The DIR is composed of three parts, Directory Information Base (DIB), DSAs and DUAs, illustrated in Figure 8.
- 4.2.3 The general DIB is organised into a tree-shaped hierarchy, the Directory Information Tree (DIT). The DIT may contain shared data replicated between DSAs (shadowing), shared data referenced by other DSAs (chaining), references to data stored on other DSAs (chaining / referrals) and local data not shared with other DSAs.
- 4.2.4 The ATN Directory Service is a specific profile of the general Directory Service specified in ISO/IEC 9594 | ITU-T Recommendation X.500 [34], including ATN-specific schema elements.



**Figure 8: General Directory Architecture**

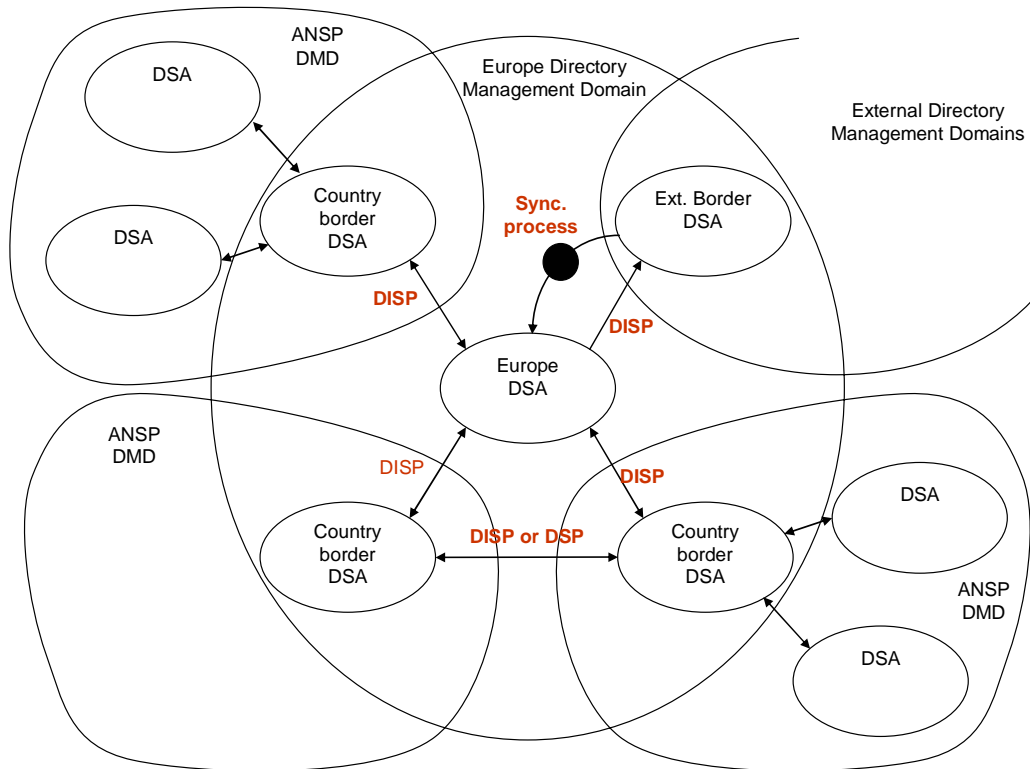
- 4.2.5 A possible architecture that can be considered for Directory Services deployment in the EATMN is illustrated in Figure 9. It comprises a set of DSAs grouped in Directory Management Domains (DMD): one for each State or Organisation and one for the common shared data. Each State/Organisation DMD is composed of at least one Border DSA that exports “public” data and retrieves “public” data from other States or Organisations or the DMD containing common shared data.

- 4.2.6 All “public” data exported by each state or organisation is centralised in a common European database facility (part of the AMC). The role of this facility is to:
- collect shared information from participating States/Organisations,
  - collect shared information relating to States/Organisations outside of the EATMN,
  - collect information from ICAO repositories related to global AMHS deployments,
  - check consistency of the collected information,
  - provide exploitable data to participating States/Organisations.



**Figure 9: Initial Directory architecture**

- 4.2.7 In order to benefit from shadowing and chaining functionalities of the X.500-based directory, the replacement of the central database by a European DSA may be considered for future deployments, as illustrated in Figure 10.



**Figure 10: Future Directory architecture**

### 4.3 Directory System Protocols

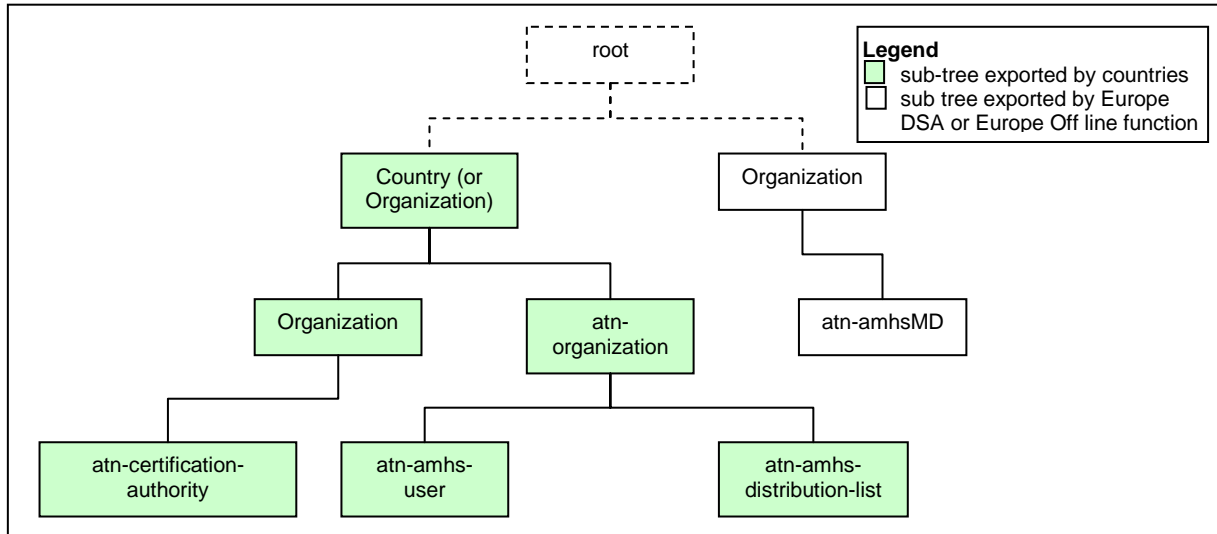
- 4.3.1 The Directory standards define several different system protocols - the Directory System Protocol (DSP), the Directory Information Shadowing Protocol (DISP), and the Directory Operational Binding Protocol (DOP).
- 4.3.2 DSP supports chaining, where a request that cannot be resolved by a DSA is passed to another DSA, and referrals, where a request that cannot be resolved by a DSA returns a reference to another DSA. ICAO Doc 9880 Part IVA [7] specifies DSP for use in the ATN.
- 4.3.3 DISP supports replication of information between DSAs. ICAO Doc 9880 Part IVA [7] provides indications for usage, but does not define a detailed DISP profile. The implementation of DISP is optional.
- 4.3.4 Note that while DISP implementation is optional, it could be useful to support automatic information updates when authorised by an administrator.
- 4.3.5 DOP is considered out of scope.

## 4.4 Directory Access

- 4.4.1 If the ATN Directory is implemented, access to directory information is via the standard X.500 Directory Access Protocol (DAP), which is the only access protocol specified in ICAO Doc 9880 Part IVA [7].
- 4.4.2 DAP may be used with an OSI lower layer stack, or with a TCP/IP mapping, which is the recommended approach in the EATMN.
- 4.4.3 LDAP is the IETF equivalent of X.500 DAP. It can provide most (but not all) of the services that DAP provides. LDAP is only an access protocol, whereas X.500 defines a complete directory system, with features such as replication, which will be important to ATS systems. There will be situations where use of both DAP and LDAP will be desirable. However, LDAP is not currently included in the ICAO specifications [7] and is therefore out of scope of this EUROCONTROL Specification, though not precluded for local directory access.

## 4.5 Directory Schema

- 4.5.1 The DIT subtree that may be exported to other DSAs has the following structure (see Figure 11: DIT Structure):
1. The root entry (level 0) of the exported subtree is a “country” or “organization” object-class, with Relative Distinguished Name (RDN) being the iso-3166-alpha2 code of the owner ANSP (e.g. C=FR) or the name of the international organisation (e.g. O=Eurocontrol).
  2. The next level (level 1) of the exported subtree contains:
    - a. an “*organization*” object-class with the RDN O=CA;
    - b. if the country supports the CAAS then this level also contains a list of “*atn-organization*” objects; one for each ICAO location. Their RDNs (attribute *atn-facility-name*) are the location indicators defined in ICAO Doc 7910 [30].
    - c. if the country supports XF addressing then this level may also contain an “*atn-organization*” object-class with the RDN O=AFTN. (The use of the ATN organisation O=AFTN for XF Countries seems to make sense following the same schema approach, especially for the user capability function).
  3. The subordinate level (level 2) associated to the “*organization*” object-class with the RDN O=CA contains an “*atn-certification-authority*” object-class.
  4. The subordinate level (level 2) associated to the “*atn-organization*” object-class contains “*atn-amhs-user*” and “*atn-amhs-distribution-list*” object-classes.



**Figure 11: DIT Structure**

4.5.2

The following diagram illustrates an example directory content for the country “France”. This is a fictitious example for illustration only. It may be updated by an actual operational version of the schema in the future. The example directory structure is composed of:

- Public data exported to other ANSPs;
- Public data imported from other ANSPs and central directory;
- Local private data filtered with chop shadowing mechanism (users from national airport);
- Local private data used to store DSA and Gateway configuration.

ROOT

*Organization*  
**O=ICAO-MD-Registry**

**Data shadowed from Central directory**

*atn-amhsMD*  
**common-name=France**  
atn-global-domain-identifier=</C=XX/A=ICAO/P=FRANCE>  
atn-icao-designator=LF  
atn-amhsMD-naming-context=<C=FR>  
atn-amhsMD-addressing-scheme=caas

*atn-amhsMD*  
**common-name=Germany**  
atn-global-domain-identifier=</C=XX/A=ICAO/P=GERMANY>  
atn-icao-designator=ED  
atn-amhsMD-naming-context=<C=DE>  
atn-amhs-addressing-scheme=caas

*Country*  
**C=FR**

**Data exported to other countries DSAs**

*Organization*  
**O=CA**

*atn-certification-authority*  
cACertificate=...  
authorityRevocationList=...  
certificateRevocationList=...  
...

*atn-organization*  
**O=LFCI**  
atn-facility-name=LFBO

*atn-amhs-user*  
mhs-or-addresses=</C=XX/A=ICAO/P=FRANCE/O=LFBO/OU=LFCI/CN=LFCIZPZX>  
atn-AF-address=LFICIZPZX  
...

*atn-organization*  
**O=LFXL**  
atn-facility-name=LFEE

*atn-amhs-user*  
mhs-or-addresses=</C=XX/A=ICAO/P=FRANCE/O=LFEE/OU=LFXL/CN=LFXLZPZX>  
atn-AF-address= LFXLZPZX  
...

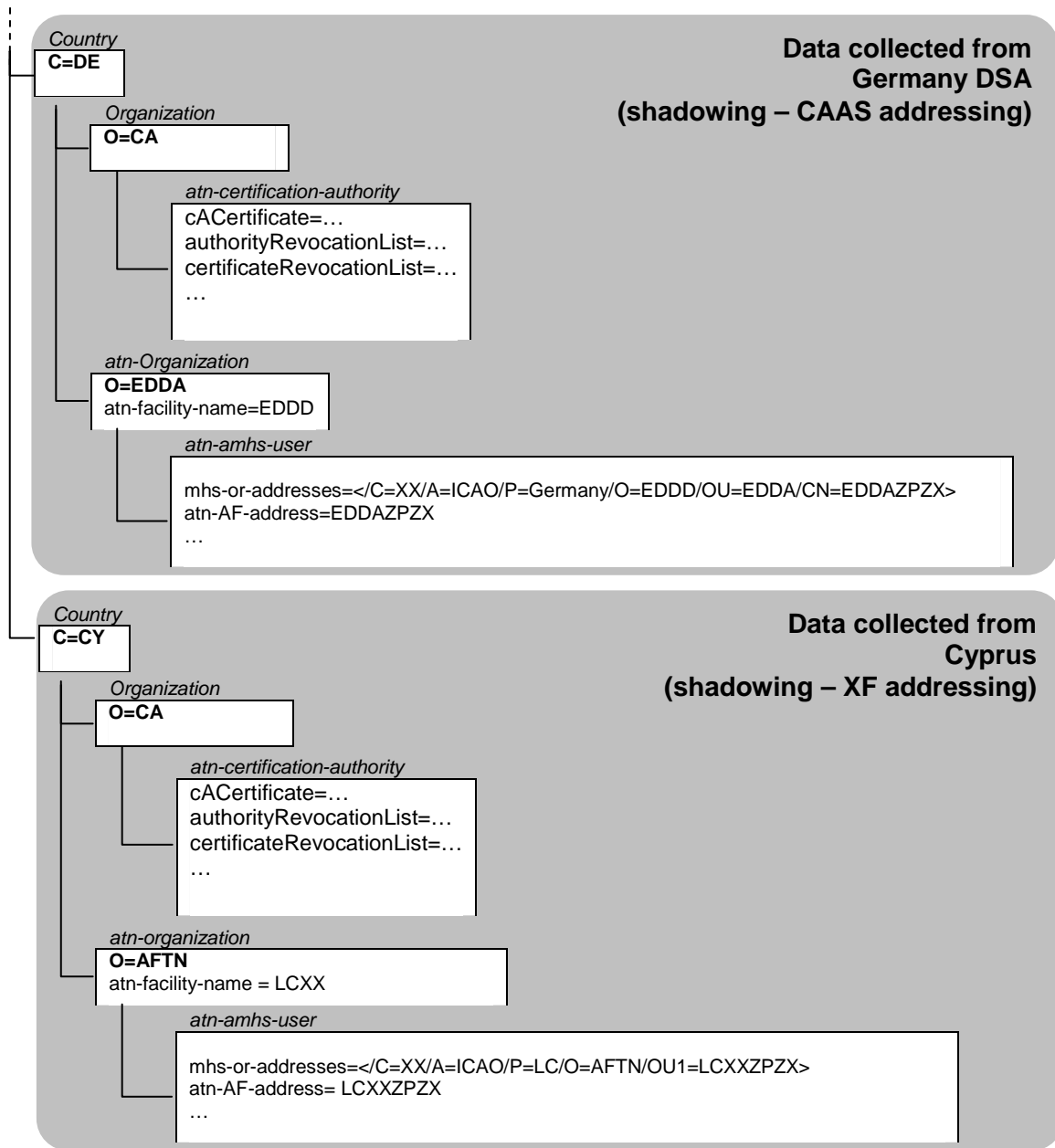
**Data not exported (e.g. users from national airport)**

*SecurityObject*  
**CN=dsa**  
...

*OrganizationUnit*  
**ou=MHS**  
...

**Private data (e.g. DSA, Gateway configuration)**





## 4.6 Versioning and Data Life Cycle

- 4.6.1 Currently, the AMC is responsible for distributing ATS messaging management information updates at regular intervals based on the AIRAC cycle. Thus, different versions of the information may exist at different times. For the time being, it is assumed that version control of the directory information is a local matter, to be managed by the local directory system administrator in the framework of common AMC procedures. In the future, specific directory attributes supporting version control may be specified.

## 4.7 Use of Directory to determine AMHS Recipient Capabilities

4.7.1 The technical provisions in ICAO Doc 9880 do not explain how to use the Directory to determine which elements of the Extended ATSMHS are supported by a recipient. Various approaches are possible, including the following:

- a) Recipient capabilities can be “known” in advance by bilateral agreement. For example, direct host (application) AMHS users would send only to agreed pre-configured addresses, with compatible capability level.
- b) It is possible to use the existing Directory schema, specifically the **BOOLEAN** attribute *atn-ipm-heading-extensions* to determine user capabilities, as follows:

IHE supported – if the ‘*atn-ipm-heading-extensions*’ attribute is **TRUE**;

FTBP supported – if the ‘*mhs-exclusively-acceptable-eits*’ attribute includes the file transfer value ‘{joint-iso-itu-t(2) mhs(6) ipms(1) eit(12) file-transfer(0)}’;

SEC supported – a sending UA does not need to know this, as a recipient that does not support security simply ignores the security features of a message (because they are in envelope extensions marked ‘non-critical’). If the sender needs to know that the recipient lacks the means to verify signatures, this could be achieved by including in a given AMHS-user application specification the requirement that an AMHS user must send a signed reply whenever it receives a signed message; the lack of a reply would indicate lack of security capability for that recipient.

4.7.2 Interoperability will only be achieved if all systems make the same assumptions and configure directories in the same way.

4.7.3 The ICAO documentation allows an implementation of an ATS Message User Agent or of an ATS Message Server to claim conformance to either the Basic ATSMHS or one of the defined subsets of the Extended ATSMHS. This EUROCONTROL Specification simplifies the subsetting problem by reducing the options to Configuration IX {Basic + IHE + DIR + FTBP} (see 3.3.6 above).

4.7.4 Therefore, any European system recipient with the ‘*atn-ipm-heading-extensions*’ attribute set to **TRUE** will support both IHE and FTBP functional groups.

## 5. AMHS SECURITY

### 5.1 General

5.1.1 This chapter contains background and explanatory material for the use of Security services in the Extended ATSMHS. A set of related technical provisions are specified in Annex D for information.

*Note: It is recognised that the provision of AMHS Security services is not as advanced as other elements of the Extended ATSMHS. For that reason, the specifications in Annex D are to be considered as advisory indications of the evolutionary direction, whose implementation is not required for compliance to this version of the EUROCONTROL Specification. However, ANSPs are encouraged to prepare the referenced end-to-end security policy as soon as possible. Further, there is a general recommendation that ATS Message Server implementations can accept and transparently relay the relevant security-related fields without causing systems to fail.*

5.1.2 Support of the AMHS Security (SEC) functional group is part of the Extended ATSMHS. ICAO Doc 9880 Part IIB [5] section 2.2.3.2 requires an end-to-end security policy to be implemented which provides message origin authentication, content integrity and message sequence integrity.

*Note: It must be recognised that the technical end-to-end message security mechanisms specified in ICAO Doc 9880 Part IIB [5] are only one part of the overall security architecture. Other elements such as virus protection, firewalls, DMZs, IPsec, etc. are equally important and must be addressed in operational ATS messaging systems.*

5.1.3 Use of the AMHS Security functionality enables a message recipient to have a very high level of confidence that a received message has not been corrupted in transit or modified accidentally or deliberately. It also provides a very high degree of confidence that the message does come from the claimed originator, who is known and trusted.

5.1.4 A message recipient can verify that the message was indeed addressed to that recipient, thereby allowing mis-delivery protection.

5.1.5 The importance of these security functions depends upon the nature of the information being transmitted in the message and the potential consequences of misdelivery, modification or masquerade.

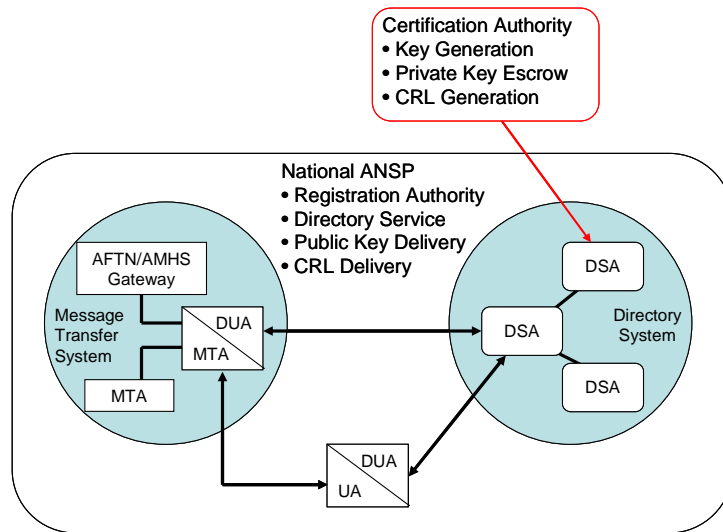
5.1.6 ICAO Doc 9880 Part IIB [5] indicates support for message sequence integrity but does not specify how message sequence numbers are assigned and verified. This would need to be specified in supporting material, or in bilateral agreements. Support for message sequence integrity using sequence numbers in the message token is not required. (The AFTN/AMHS Gateway

supports sequence integrity by other means; see ICAO Doc 9880 Part IIB [5] section 4.5.2.4.15.b.1.iii).

- 5.1.7 As in ICAO Doc 9880 Part IIB [5], implementation of content confidentiality is not mandatory.
- 5.1.8 To support content integrity, a recipient must be provided with tools to verify that the content of a message has not been modified during the transfer process.
- 5.1.9 To support message origin authentication, a recipient must be provided with tools to confirm the identity of the sender of the received message.
- 5.1.10 Some security provisions are also available at the lower layers. However, this does not provide end-to-end assurance between end users.

## **5.2 AMHS Security Framework**

- 5.2.1 In the Basic ATSMHS, the security at each AMHS End System is deemed a local issue to be addressed by the authority in charge of the system. ICAO Doc 9880 Part IIB [5] recommends, in 2.2.3.1, that security in the Basic ATSMHS be obtained by procedural means rather than by technical features inherent to the AMHS.
- 5.2.2 In the Extended ATSMHS, the general AMHS security provisions aim at protecting ATS Message exchanges against the identified threats, namely masquerade, modification and replay.
- 5.2.3 The security model in ICAO Doc 9880 Part IIB [5] §2.2.3 is fully applicable when AMHS Security services are implemented.
- 5.2.4 In the AMHS security architecture, a digital signature is transferred end-to-end along with the message, and the format of the message being transferred is not affected. This means that AMHS security can be added with minimal disruption to a deployment that does not use the security features, provided that the ATS message transfer service transparently relays the required elements of service.
- 5.2.5 One possible architecture of an AMHS implementation is illustrated in Figure 12, in which the Directory service is used in support of the delivery of security elements.



**Figure 12: Global AMHS Architecture including CA**

### 5.3 Public Key Infrastructure

- 5.3.1 To overcome the issues associated with secure distribution of cryptographic keys, a public key infrastructure (PKI) is assumed if AMHS Security services are implemented. The PKI is used to distribute public keys via certificates signed by a trusted certificate authority (CA). Each State implementing AMHS Security needs access to a CA; the same CA may be shared by several States.
- 5.3.2 When using AMHS Security functions, sending ATS Message User Agents derive a digital signature from the message content using a private signing key. Recipient ATS Message User Agents validate the signature using the public key of the sender.
- 5.3.3 The recipient needs to know the CA's public key in order to verify the certificate containing the originator's public key. Verifying the originator's certificate is the core function of PKI. For simple deployment with a single CA, the originator and recipient use the same CA, and the recipient is configured to trust certificates issued by its own CA and thus will trust the originator's certificate.
- 5.3.4 In the model where originator and recipient have different CAs, it is necessary for CAs to cross-certify either with each other, or with a common "bridge" CA, in order for the message recipient to be able to trust the received certificate.

## **6. ADDITIONAL AMHS REQUIREMENTS**

### **6.1 Testing and Verification**

- 6.1.1 In order to demonstrate compliance with this EUROCONTROL Specification, a suite of test cases with appropriate test coverage must be successfully executed. A description of the tests would form part of the EC declaration of conformity.
- 6.1.2 ICAO EUR Doc 020 [8] specifies in Appendices C through F a set of testing requirements, conformance, interoperability and pre-operational tests covering the Basic ATSMHS requirements. There is the need to augment the test coverage in such a way as to include the additional functionality of the relevant elements of the Extended ATSMHS.

## **7. TRANSITION / COEXISTENCE ISSUES**

### **7.1 AFTN to AMHS Transition**

- 7.1.1 As a first step, the Basic ATSMHS can be deployed across Europe simply to replace AFTN, in compliance with ICAO Regional requirements endorsed by EANPG. Subsequently, it is envisaged that ANSPs will continue to implement other elements of the Extended ATSMHS.
- 7.1.2 As aging AFTN switches are replaced with ATS Message Servers, AFTN end users will become AMHS indirect users, supported by the AFTN/AMHS Gateway.
- 7.1.3 The ultimate goal is to phase out the AFTN terminal equipment in favour of ATS Message User Agents. At this stage, all users will be AMHS direct users. The AFTN/AMHS Gateways can only be decommissioned when all indirect users connected to the switch (terminals and applications) are migrated to AMHS. Note that such decommissioning depends also on the migration of all communicating EATMN countries from AFTN to AMHS.
- 7.1.4 Systems sending and receiving AFTN messages must be considered. As long as these systems expect AFTN formatted messages, the AFTN/AMHS Gateways will have to remain.
- 7.1.5 There are a number of transition steps to achieving this end state. Timescales for migration and transition are outside the scope of this EUROCONTROL Specification.
- 7.1.6 The migration from AFTN/CIDIN to AMHS requires the development of AMHS Operational Procedures, to ensure that transition steps are performed smoothly and without service disruption.
- 7.1.7 Common facilities, and specifically the routing management function, are of utmost importance to the performance of these AMHS Operational Procedures. It is one of the main goals of the AMC to provide support to the transition to AMHS.
- 7.1.8 AMHS procedures for migrating from AFTN to AMHS are included as Appendix A to ICAO EUR Doc 021 [9], which defines the procedure for the introduction of a new AMHS COM Centre in the ICAO EUR/NAT AMHS network.
- 7.1.9 During transition from AFTN/CIDIN to AMHS, existing AFTN/CIDIN routes will be "concatenated" with direct AMHS routes in AMHS Gateways at the borders between the remaining AFTN/CIDIN and the growing AMHS islands.
- 7.1.10 ICAO EUR Doc 021 [9] provides guidance in this area.

## **7.2 Basic ATSMHS to Extended ATSMHS Transition**

7.2.1 The Basic ATSMHS may be implemented as a transition step to full Extended ATSMHS. ICAO Doc 9880 Part IIB [5] notes:

*It is intended that eventually the Extended ATS Message Handling Service will be supported by all ATS Message Handling Service users, so that the Basic ATS Message Handling Service will not be required anymore. However the latter may be maintained for transition purposes as long as required.*

7.2.2 Coexistence between the two levels of service is facilitated by the use of Directory service by users of the Extended ATSMHS, to determine the capabilities of intended message recipients.

## **7.3 Deployment of Directory**

7.3.1 At present, updates to European ATS messaging configuration and addressing information are published each AIRAC cycle and distributed by the AMC using procedures described in ICAO EUR Doc 021 [9].

7.3.2 As DSAs become deployed in Europe, AMHS address and capability information which is stored in the Directory can be distributed using these same procedures.

7.3.3 In the final state, migration to allow synchronisation with a highly available and secure centralised directory system in the AMC can be envisaged. This would ensure information consistency throughout the EATMN and avoid complex many-to-many synchronisation relationships.

7.3.4 Transition from the current procedures towards the final state needs to be carefully managed.



## **8. TRACEABILITY TO REGULATORY PROVISIONS**

### **8.1 Implementation Conformance Statements**

8.1.1 This EUROCONTROL Specification provides means of compliance to SES regulatory material and each Annex includes a section describing relevant conformity assessment materials. These include implementation conformance statement (ICS) templates, which allow the level of compliance with the specification to be recorded. In many cases, the ICS is included by reference to other documents.

8.1.2 The ICS templates are intended to support clear statements of:

- a) conformity or non-conformity with the requirements ('shall' items) of the specification;
- b) any reasons or mitigations in the case of declaration of non-conformity.

8.1.3 The ICS template also allows the degree of conformity with recommended items ('should' statements) to be described.

8.1.4 The Annexes of this EUROCONTROL Specification provide separate ICS templates for various functional elements of the specification. This structure facilitates the possible future definition of additional means of compliance (MOC) for any of the separate functional areas without impacting the other functional areas. For example, support for alternative security algorithms or directory schemas could be defined as requirements or technology evolve. Each Annex therefore constitutes a "MOC element".

8.1.5 Completed ICS can be used in support of the EC declaration of conformity and/or part of Technical File accompanying the EC declaration of verification.

### **8.2 Traceability to SES Essential Requirements**

8.2.1 Essential requirements applicable to systems within the EATMN are categorised in Annex II of the interoperability Regulation [1].

8.2.2 For the purpose of the interoperability Regulation [1], the EATMN is subdivided into eight types of system. The systems and procedures of greatest relevance to this EUROCONTROL Specification are identified in Annex I of the interoperability Regulation [1] as:

- *Communications systems and procedures for ground-to-ground, ( ... ) communications.*

8.2.3 Also relevant, insofar as they may interface to the AMHS as direct "host" users, are:

- *Systems and procedures for ATS, in particular flight data processing systems, [and] surveillance data processing systems (...).*

8.2.4 Appendix 1 provides traceability tables between the SES essential requirements and the provisions of this EUROCONTROL Specification.

## 9. DOCUMENT UPDATE PROCEDURES

- 9.1.1 This is a living document. It may be updated, after operational validation. It is also expected to evolve following real project and field experience, as well as advances in the technology state-of-the-art. If in future, potential changing/emerging needs derived from aeronautical requirements appear in the current applications, subsequent analysis for the ad-hoc specific functionality will have to be performed, if appropriate. Updates will follow EUROCONTROL Notice of Proposed Rule Making (ENPRM) procedures<sup>4</sup> using the process outlined in this section.
- 9.1.2 This document is subject to continuous review and improvement by all ATM Stakeholders including Industry, through the EUROCONTROL OneSky Online site (<https://extranet.eurocontrol.int>). This arrangement will allow active participation and objective feedback from all partners.
- 9.1.3 The main objectives of the continuous review are:
- To improve the quality of the requirements (e.g. clarity, testability, etc.);
  - To verify that the level of detail published is adequate;
  - To ensure that design oriented requirements, imposing unnecessary constraints to technical solutions, have been avoided;
  - To ensure that the evolving state of the art is properly reflected;
  - To have the supplying industry aware of the developments and directions in ATM systems and prepared to cover and supply the appropriate systems.
- 9.1.4 It is necessary to periodically check this EUROCONTROL Specification for consistency with referenced material, notably ICAO international and regional SARPs and manuals.
- 9.1.5 The update process for this EUROCONTROL Specification may be summarised as follows:
1. All change proposals and issued changes to referenced documents will be checked in detail by an Impact Assessment Group. An Impact Assessment Report will be generated for consideration by the Specification Drafting Group (SDG).
  2. The SDG will compose a new Internal Draft to propose changes covering the impact assessment for internal discussion.
  3. The new Internal Draft will be assessed for conformance against the regulations, any relevant ICAO policies and safety considerations.
  4. If necessary further Internal Drafts will be produced.

---

<sup>4</sup> ENPRM procedures are defined in [www.eurocontrol.int/enprm](http://www.eurocontrol.int/enprm)

5. After the SDG has finalised the updates a new Intermediate Draft will be issued for review by stakeholders in accordance with ENPRM mechanisms. Workshops may need to be arranged depending on how extensive and significant the changes are.
6. Following the reception of comments further Intermediate Drafts will be produced as necessary and distributed for confirmation of correct update.
7. Following a suitable period for further response, assuming that no objections have been raised, the resulting draft will be upgraded to the new Baseline Version. Approval and document change record sections will be updated accordingly. A date will be negotiated with stakeholders and set for applicability of the revised facilities. The new baseline document will be considered to be in force from that date onwards.
8. Where appropriate, a recommendation will be made to the European Commission to update the reference in the Official Journal of the European Union to recognise this new version as a Community specification acceptable for compliance with the EC Regulations.

## **10. LIST OF REFERENCES**

### **10.1 Description of References**

- 10.1.1 This EUROCONTROL Specification incorporates by reference a number of specifications and standards maintained by ICAO, EUROCAE and ETSI. In turn, these documents also reference many ISO/IEC, ITU-T and IETF standards. A list of the current versions of these standards is provided for information in Appendix 2.
- 10.1.2 Primary references are those referred to in the requirements of, and which therefore constitute an integral part of, this EUROCONTROL Specification.
- 10.1.3 Associated references are those standards and other documents which are referenced from recommendations or explanatory material and are therefore not essential for implementation.

### **10.2 Primary References**

- [1] Regulation (EC) No 552/2004 of the European Parliament and of the Council of 10 March 2004 on the interoperability of the European Air Traffic Management network (the interoperability Regulation), OJ L 96/26, 31.3.2004
- [2] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, OJ L 13, 19.1.2000, p. 12–20
- [3] ICAO Convention on International Civil Aviation, Annex 10 — Aeronautical Telecommunications, Volume II — Communication Procedures including those with PANS status, Sixth edition – October 2001, incorporating Amendment 83 (20/07/2008)
- [4] ICAO Convention on International Civil Aviation, Annex 11 – Air Traffic Services, Thirteenth edition - July 2001, incorporating Amendment 45 (16/07/2007)
- [5] ICAO Doc. 9880-AN/466 Manual on Detailed Technical Specifications for the Aeronautical Telecommunication Network (ATN) using ISO/OSI standards and protocols, Part IIB – Ground-Ground Applications – ATS message handling service (ATSMHS), 1st edition (unedited), December 2007
- [6] [ATN SEC] ICAO Doc. 9705-AN/956 – Manual of Technical Provisions for the Aeronautical Telecommunications Network (ATN) Third Edition (2002), Sub-Volume VIII – ATN Security.
- [7] [ATN DIR] ICAO Doc 9880-AN/466 – Manual on Detailed Technical Specifications for the Aeronautical Telecommunication Network (ATN) using ISO/OSI standards and protocols, Part IVA – Directory Services, 1<sup>st</sup> edition (unedited)

- [8] ICAO EUR Doc 020 EUR AMHS Manual, Version 4.0 (April 2009)  
[http://www.paris.icao.int/documents\\_open/files.php?subcategory\\_id=74](http://www.paris.icao.int/documents_open/files.php?subcategory_id=74)
- [9] ICAO EUR Doc 021 ATS Messaging Management Manual, Version 5.0 (May 2009) [http://www.paris.icao.int/documents\\_open/files.php?subcategory\\_id=78](http://www.paris.icao.int/documents_open/files.php?subcategory_id=78)
- [10] ICAO EUR Doc 022 AFS Security Guidelines, AFSG Planning Group, Version 1.0 (April 2008)  
[http://paris.icao.int/documents\\_open/files.php?subcategory\\_id=88](http://paris.icao.int/documents_open/files.php?subcategory_id=88)
- [11] EUROCAE Document ED-78A, Guidelines for Approval of the Provision and use of Air Traffic Services supported by Data Communications, December 2000
- [12] EUROCAE Document ED-111, Functional Specifications for CNS/ATM Ground Recording, July 2002 including Amendment 1 (30/07/2003)
- [13] ETSI EG 201 057 v1.1.2 (1997-07) Telecommunication security; Trusted Third Parties (TTP); Requirements for TTP services.
- [14] ETSI TS 101 456 v1.4.3 (2007-05) Electronic Signatures and Infrastructures (ESI) Policy Requirements for certification authorities issuing qualified certificates.
- [15] FIPS PUB 180-2 Federal Information Processing Standards Publication - Secure Hash Signature Standard (SHS) (August 2002)  
<http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf>
- [16] ISO/IEC ISP 15126-1:1999 Information technology - International Standardized Profiles FDY1n –Directory Data Definitions – Part 1: FDY11 – Common directory use (normal)
- [17] ISO/IEC ISP 11189 Information technology -- International Standardized Profile FDI2 - Directory Data Definitions - MHS Use of the Directory, Edition 1 (1997) [WITHDRAWN IN 2007]
- [18] ISO/IEC 10021-n Information technology - Message Handling Systems (MHS) – (multi-part Standard) Edition 2 (2003) (alternatively ITU-T X.400 Series of Recommendations)
- [19] ISO/IEC ISP 10611-n:2003 Information technology - International Standardized Profiles AMH1n -- Message Handling Systems - Common Messaging (multi-part Standard), Edition 3 (2003)
- [20] ISO/IEC ISP 12062-n:2003 Information technology - International Standardized Profiles AMH2n - Message Handling Systems - Interpersonal Messaging - (multi-part Standard), Edition 3 (2003)
- [21] IETF RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (November 2003)
- [22] ICAO Doc 9896-AN/469 Manual for the ATN using IPS Standards and Protocols, 1<sup>st</sup> edition (unedited)

### 10.3 Associated References

- [23] Regulation (EC) No 549/2004 of the European Parliament and of the Council of 10 March 2004 laying down the framework for the creation of the single European sky (the framework Regulation), OJ L 96/1, 31.3.2004
- [24] Commission Regulation (EC) No 482/2008 of 30 May 2008 establishing a software safety assurance system to be implemented by air navigation service providers and amending Annex II to Regulation (EC) No 2096/2005, OJ L 141/5, 31.5.2008
- [25] Commission Regulation (EC) No 2096/2005 of 20 December 2005 laying down common requirements for the provision of air navigation services, OJ L 335/13, 21.12.2005
- [26] [ATN SARPs] ICAO Convention on International Civil Aviation, Annex 10 — Aeronautical Telecommunications, Volume III, — Communication Systems, Second Edition — July 2007, incorporating Amendment 83 (20/11/2008), ISBN 92-9194-953-1, Part I — Digital Data Communication Systems, Chapter 3 — Aeronautical Telecommunication Network (ATN).
- [27] Routing Directory for COM Centres in the EUR/NAT Regions, Part I — Documentation. Overview, Explanations, Procedures, ICAO AFSG Operations Group
- [28] ICAO Register of AMHS Management Domains  
<http://www.icao.int/anb/panels/acp/amhs/amhs.cfm>
- [29] ICAO Convention on International Civil Aviation, Annex 17 — Security, 8th edition - April 2006, Reprinted August 2007, incorporating Amendments 1–11. ISBN 92-9194-949-3
- [30] ICAO Doc 7910 – Location Indicators – 131<sup>st</sup> edition, March 2009 ISBN 978-92-9231-280-0, ISSN 1727-2610 (New edition quarterly)
- [31] EUROCAE Document ED-109, Guidelines for CNS/ATM Systems Software Integrity Assurance., March 2002
- [32] ETSI TR 102 040 v1.2.1 (2004-02) International Harmonization of Policy Requirements for CAs issuing Certificates
- [33] ETSI TS 102 176-1 v2.0.0. (2007-11) Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms.
- [34] ISO/IEC 9594-n Information technology - Open Systems Interconnection - The Directory, (multi-part Standard) Edition 5 (2005) (alternatively ITU-T X.500 Series of Recommendations)
- [35] ISO/IEC 9594-8:2005 | ITU-T Recommendation X.509 (08/2005) Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks.
- [36] ISO/IEC 8825-1:2002 | ITU-T Recommendation X.690 (07/2002) Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)

- [37] [ECIP] European Convergence and Implementation Plan, Years 2008-2012, EATM Information Centre reference: 07/06/29-38 (July 2007)
- [38] X/Open Technical Standard "API to Electronic Mail (X.400)" Issue 2 (available from The Open Group)
- [39] [LDAP] IETF RFC 4510 Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map, K. Zeilenga, Ed. (June 2006)
- [40] [SNMP] IETF RFC 3411 (STD 062) An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks, D. Harrington, R. Presuhn, B. Wijnen (December 2002)
- [41] [OCSP] IETF RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams (June 1999)
- [42] IETF RFC 2849 The LDAP Data Interchange Format (LDIF) – Technical Specification, G. Good (June 2000)
- [43] NATO Standardization Agreement (STANAG) No 4406 – Military Message Handling System (MMHS), Edition 2 (October 2006)
- [44] EUROCONTROL ATM Strategy for the Years 2000+ (July 2003)
- [45] EUROCONTROL Civil-Military CNS/ATM Interoperability Roadmap (January 2006)
- [46] SESAR Master Plan – SESAR Definition Phase Deliverable 5, SESAR Consortium DLM-0710-001-02-11 (April 2008)
- [47] IETF RFC 2789 Mail Monitoring MIB. N. Freed, S. Kille. (March 2000)



**EUROCONTROL SPECIFICATION  
on the  
Air Traffic Services Message  
Handling System (AMHS)  
ANNEX A – Basic Service**

**SPECIFICATION DOCUMENT IDENTIFIER: EUROCONTROL-SPEC-0136**

<b>Edition Number</b>	<b>:</b>	<b>2.0</b>
<b>Edition Date</b>	<b>:</b>	<b>18/09/2009</b>
<b>Status</b>	<b>:</b>	<b>Released</b>
<b>Intended for</b>	<b>:</b>	<b>General Public</b>
<b>Category</b>	<b>:</b>	<b>EUROCONTROL Specification</b>

## DOCUMENT CHANGE RECORD

The following table records the complete history of the successive editions of the present document.

EDITION NUMBER	EDITION DATE	INFOCENTRE REFERENCE	REASON FOR CHANGE	PAGES AFFECTED
0.1	16/01/08		Initial outline	All
0.2	25/01/08		Detail added	All
0.3	26/02/08		Further evolution. Input to Drafting Group	All
0.4	01/04/08		Further evolution. Requirements from GESS added.	All
0.5	13/06/08		Draft for Review Group	All
0.6	24/10/08		Updated and restructured after informal stakeholder review. Annex A split into 2 – Basic & Extended	All
1.0	08/12/08		Updated after informal stakeholder review. Input to formal consultation.	All
1.1	27/07/09		Updated after ENPRM-09/001 formal consultation.	All
2.0	18/09/09		Released Issue	Footers

## CONTENTS

<b>ANNEX A - SPECIFICATION OF BASIC INTEROPERABILITY REQUIREMENTS .....</b>	<b>1</b>
A.1 CONFIGURATION CONTROL .....	1
A.2 REQUIREMENTS AND EXPLANATORY MATERIALS .....	2
A.2.1 Common Requirements .....	2
A.2.1.1 Standards Baseline .....	2
A.2.1.2 General Requirements .....	3
A.2.1.3 Safety Requirements .....	3
A.2.1.4 Performance Requirements .....	5
A.2.1.5 Naming and Addressing .....	6
A.2.1.6 Logging .....	6
A.2.1.7 Availability, Reliability, Maintainability .....	6
A.2.1.8 System Operation and Management .....	7
A.2.1.9 Transitional Procedures .....	9
A.2.2 ATS Message Server Requirements .....	9
A.2.2.1 EATMN Boundary Requirements .....	10
A.2.3 ATS Message User Agent Requirements .....	11
A.2.4 Message Store Requirements .....	12
A.2.5 AFTN/AMHS Gateway Requirements .....	12
A.3 CONFORMITY ASSESSMENT MATERIALS .....	14
A.3.1 Compliance Statement .....	14
A.3.2 Testing Requirements .....	18



## ANNEX A – SPECIFICATION OF AMHS BASIC INTEROPERABILITY REQUIREMENTS

### A.1 CONFIGURATION CONTROL

#### A.1.1 MOC ELEMENT IDENTIFICATION

MOC_Title	MOC_Version	MOC_Edition
AMHS_BAS_IOP	1	1

#### A.1.2 MOC ELEMENT CHANGE RECORD

The following table records the complete history of the successive editions of MOC specifications.

Version Number	Edition Number	Edition Date	Reason for Change	Sections Affected
1	1	18/09/09	Initial specification	All

#### A.1.3 MOC ELEMENT TRACEABILITY TOWARDS REGULATORY PROVISIONS

The following table records the traceability history of regulatory provisions associated with this MOC element.

Version Number	Edition Number	Implementing rule references	References of regulatory provisions	Validation date
1	1	N/A	Regulation (EC) No 552/2004 [1] Annex II Part A and Part B (4) - Essential requirements applicable to communications systems and procedures for ground-to-ground communications	

#### A.1.4 MOC ELEMENT TRACEABILITY TOWARDS INTERNATIONAL STANDARDS

The following table records the traceability of international standards associated with this MOC element.

International standards identification	References of text parts used to derive MOC specifications	Standards text incorporated by reference into the MOC element
ICAO Doc 9880 Part IIB [5]	(Basic ATSMHS only)	
ICAO EUR Doc 020 [8]		Whole document
ICAO EUR Doc 021 [9]		Whole document

## A.2 REQUIREMENTS AND EXPLANATORY MATERIALS

*Note 1: This normative Annex is an integral part of this EUROCONTROL Specification. It specifies requirements for AMHS End Systems that support the Basic ATSMHS as defined in ICAO Doc 9880 Part IIB [5].*

*Note 2: This Annex must be read in conjunction with the Main Body of this EUROCONTROL Specification, which provides definitions, document references and contextual information. References given in square brackets are defined in section 10 of the Main Body.*

*Note 3: The Basic ATSMHS is intended as a transition step providing interoperability with existing AFTN equipment and supporting the migration from AFTN to AMHS technology. As such, it supports existing data flows and concepts of operation for applications based on the interchange of ATS messages.*

*Note 4: The Basic ATSMHS provides only for the exchange of simple text messages, including a formatted ATS Message Header field. It does not support new concepts of operation requiring the general exchange of binary data or files and does not provide strong authentication or data integrity services. Further, the Basic ATSMHS does not benefit from a standardised directory function, which in the Extended ATSMHS can be used to enhance seamless operation by ensuring the up-to-date dissemination of address and configuration information.*

*Note 5: This Annex is structured such that requirements common to all AMHS End Systems are specified in section A.2.1, followed by requirements specific to each AMHS End System type. Compliance is conditional upon the type of AMHS End System under consideration (e.g. section A.2.2 on ATS Message Server is not applicable when considering requirements for ATS Message User Agents).*

### A.2.1 Common Requirements

#### A.2.1.1 Standards Baseline

**[AMHS-BAS-A01]** AMHS End Systems shall comply with the requirements identified in ICAO EUR Doc 020 [8] unless otherwise explicitly stated in this EUROCONTROL Specification.

**[AMHS-BAS-A03]** AMHS End Systems shall comply with the requirements specified in ICAO Doc 9880 Part IIB [5] applicable to the Basic ATSMHS, except where explicitly stated otherwise.

**[AMHS-BAS-A04]** In the event of conflicting requirements not explicitly identified, the specification in ICAO Doc 9880 Part IIB [5] shall take precedence.

**[AMHS-BAS-A05]** Due account shall be taken of any published defect resolutions relating to the ICAO AMHS documentation.

*Note. Any outstanding defect reports and/or amendment proposals need to be analysed when preparing an ANSP's system specification. Any that affect interoperability would be required to be implemented in the supplied system.*

**[AMHS-BAS-A06]** Implementations of AMHS Components shall conform to the 2003 version of the MHS base standards [18] and the 2003 version of the referenced International Standardized Profiles (ISPs) [19], [20].

*Note: This differs from ICAO Doc 9880 Part IIB [5], which refers to the 1990 MHS standards and the Edition 1 (1994/95) or later edition ISPs for the Basic ATS Message Handling Service, but refers to the 2003 MHS standards and the Edition 3 (2003) ISPs to define the*

*Extended ATS Message Handling Service. The European ATS Messaging Service Profile in Appendix B of ICAO EUR Doc 020 [8] refers only to the Edition 3 (2003) ISPs, and by implication to the 2003 base standards. It provides, in Appendix B Annex R, a mapping between the elements of 2003 ISPs to the corresponding elements of the earlier versions.*

**[AMHS-BAS-A07]** Compatibility with the current version of referenced standards and any relevant corrigenda should be taken into account.

#### A.2.1.2 General Requirements

**[AMHS-GEN-A01]** The AMHS shall enable the exchange of messages between the following types of users:

- direct AMHS user to direct AMHS user;
- direct AMHS user to indirect AMHS user;
- indirect AMHS user to direct AMHS user;
- indirect AMHS user to indirect AMHS user.

**[AMHS-GEN-A02]** AMHS Components shall be able to communicate using the TCP/IP Transport Service, as specified in ICAO Doc 9880 Part IIB [5], section 3.2.2.2.3.

**[AMHS-GEN-A03]** AMHS End System implementations should follow the “Guidelines for system requirements” in section 5 of ICAO EUR Doc 020 [8].

**[AMHS-GEN-A04]** Wherever possible, AMHS Component implementations should make use of common and standardised interfaces.

*Note: Such interfaces are specified in IETF RFCs or by established industry groups such as The Open Group [38].*

**[AMHS-GEN-A05]** Specifically, standardised interfaces where available for message submission, transfer and delivery, system management, etc. shall be used as a means of enhancing Interoperability between system components.

**[AMHS-GEN-A06]** AMHS End Systems should support by local means the object classes and attribute types of directory information specified in ICAO EUR Doc 020 [8] Appendix B Annex K, with a (local) mechanism to obtain such information by a UA, MTA or MTCU component.

**[AMHS-GEN-A07]** AMHS End Systems shall be capable of interworking with independent implementations of AMHS End Systems in accordance with the permissible combinations listed in ICAO Doc 9880 Part IIB [5], section 1.2.

*Note: Such interworking includes correct interoperation representing the services explicitly and implicitly requested by either end user.*

**[AMHS-GEN-A08]** AMHS End Systems supporting the Basic ATSMHS shall be designed to accommodate the evolution to support the Extended ATSMHS, e.g. by including well-defined interfaces and software hooks in areas where future extensions are foreseen.

#### A.2.1.3 Safety Requirements

*Note 1: Using the methodology of EUROCAE ED-78A [11] (Guidelines for Approval of the Provision and Use of ATS Supported by Data Communications), this EUROCONTROL Specification can be likened to an INTEROP specification. In general, it would be complemented by a detailed specification of Safety and Performance Requirements (SPR). ANSPs will have responsibility to ensure the SPR exists for each defined service.*

*Note 2: The migration from AFTN/CIDIN to AMHS requires the ANSP to prepare an "AMHS Introduction Safety Case". It is expected that a Functional Hazard Assessment (FHA) will have been performed. During the design, a preliminary System Safety Assessment (SSA) will be carried out, with a final SSA after installation.*

*Note 3: No specific safety requirements other than the general requirements common to the introduction of **any** ATS system and constituent have been identified for AMHS.*

**[AMHS-SAF-A01]** As for any EATMN system or constituent, a safety assessment shall be performed for the initial planned use of the ATSMHS.

**[AMHS-SAF-A02]** Procedures shall be put in place to ensure that a further safety assessment is performed as and when additional end-user applications making use of the ATSMHS are deployed.

**[AMHS-SAF-A03]** AMHS End Systems and operations in the EATMN shall achieve agreed high levels of safety using established safety management and reporting methodologies.

*Note: For example, the EUROCONTROL Safety Assessment Methodology and associated tools could be employed.*

**[AMHS-SAF-A04]** A harmonised set of safety requirements for the design, implementation, maintenance and operation of AMHS End Systems, both for normal and degraded modes of operation, shall be applied with a view to achieving the agreed safety levels for the entire AMHS.

*Note: ANSPs will have responsibility to cooperate to derive harmonised safety requirements for each defined service supported by AMHS.*

**[AMHS-SAF-A05]** AMHS End Systems shall be designed, built, maintained and operated, using the appropriate and validated procedures, in such a way that the tasks assigned to the control staff are compatible with human capabilities, in both the normal and degraded modes of operation, and are consistent with required safety levels.

**[AMHS-SAF-A06]** AMHS End Systems shall be designed, built, maintained and operated using the appropriate and validated procedures, in such a way as to be free from harmful interference in their normal operational environment.

#### A.2.1.3.1 Software Assurance Level

*Note. A Software Safety Assurance System complying with Regulation (EC) No. 482/2008 [24] will deal specifically with software related aspects, including all on-line software operational changes (such as cutover/hot swapping).*

**[AMHS-SAF-A07]** The allocated software assurance level shall be commensurate with the most adverse effect that software malfunctions or failures may cause, taking into account the risks associated with software malfunctions or failures and the architectural and/or procedural defences identified.

*Note 1: The ANSP is required to ensure that software requirements specify, as appropriate:*

- *The functional behaviour (normal and downgraded modes) of the ATM software,*
- *Timing performances,*
- *Capacity,*
- *Accuracy,*
- *Software resource usage on the target architecture,*



- *Robustness to abnormal operating conditions,*
- *Overload tolerance.*

*Note 2: The assurance level required will be based on the local system safety case, together with acceptable means of compliance, such as a reference to EUROCAE document ED-109 [31] Guidelines for CNS/ATM Systems Software Integrity Assurance. Note that ED-109 does not provide guidance to allocate Assurance Level. Only a part of the safety lifecycle is considered in ED-109 and no requirements are set concerning acquisition, supply, installation, acceptance, maintenance, operation and decommissioning phases as required by Regulation (EC) No 482/2008 [24].*

#### A.2.1.4 Performance Requirements

**[AMHS-PER-A01]** An operational performance assessment (OPA, as defined in EUROCAE Document ED-78A [11]) shall be performed for the initial planned use of the ATSMHS.

**[AMHS-PER-A02]** Procedures shall be put in place to ensure that a further OPA is performed as and when additional end-user applications making use of the ATSMHS are deployed.

**[AMHS-PER-A03]** The ATSMHS within the EATMN shall be such as to meet the requirements of quality of service, coverage and redundancy as required for the supported applications.

*Note: This implies that applications using the ATSMHS must have such requirements specified. For legacy AFTN applications migrating to AMHS, e.g. flight plan distribution, the minimum requirement is that the existing performance is maintained.*

**[AMHS-PER-A04]** When adding new services, the affect of the additional message traffic on the existing traffic shall be considered.

**[AMHS-PER-A05]** AMHS End Systems shall be designed, built, maintained and operated using the appropriate and validated procedures, in such a way as to achieve the required performances for a specific application, in particular in terms of:

- a) communication processing time,
- b) integrity,
- c) availability and
- d) continuity of function.

**[AMHS-PER-A06]** AMHS End Systems shall be designed and dimensioned to enable the end-to-end performance requirements for each “QoS Flow Type Class” listed in ICAO EUR Doc 020 [8], section 3.1.4, Table 1 to be met.

*Note: Testing compliance to the above requirement may require the implementation of suitable monitoring tools to enable statistical measurements of the end-to-end performance of the ATSMHS to be performed.*

**[AMHS-PER-A07]** AMHS End Systems and their constituents supporting new, agreed and validated concepts of operation shall be designed, built, maintained and operated, using appropriate and validated procedures, in such a way as to be interoperable in terms of timely sharing of correct and consistent information.

*Note: Timely sharing of information is taken to mean that the user information transported by the ATSMHS is delivered with minimal delay, consistent with the performance requirements of the individual application. The correctness of the information can be enhanced by ensuring*

*the integrity of the transported information, which will be by application-specific means for users of the Basic ATSMHS.*

**[AMHS-PER-A08]** AMHS End Systems should be capable of supporting the peak rate hour's performance, which corresponds to at least 20% of the daily traffic requirements for that AMHS End System.

**[AMHS-PER-A09]** An AMHS End System shall comply, to the extent possible, with the sizing recommendations specified in section 5.7 of ICAO EUR Doc 020 [8].

*Note: The SPACE project calculated that to support existing and foreseen traffic flows, the range of byte streams is 1.8 to 6.1 MByte per link in the peak hour, i.e. an average of 4 to 14 kilobits per second at the network layer. These figures form indicative capacity requirements for the underlying communication infrastructure.*

#### A.2.1.5 Naming and Addressing

*Note: No specific naming and addressing requirements are identified other than those specified in ICAO Doc 9880 Part IIB [5], section 2.5.*

#### A.2.1.6 Logging

**[AMHS-LOG-A01]** Data exchanges using the ATSMHS shall be recorded in accordance with the following ICAO standards applicable to the ground-based recording function of data link communications:

- Section 3.5.1.5 of ICAO Annex 10 Volume II [3];
- Section 6.2 of ICAO Annex 11 [4].

**[AMHS-LOG-A02]** EUROCAE ED-111 [12] shall be considered as sufficient means of compliance of the ground-based recording function with regard to the identified ICAO standards applicable to the ground-based recording function of ATS data communications.

**[AMHS-LOG-A03]** AMHS End Systems shall support the relevant requirements for traffic logging as described in sections 2.7, 3.2.3 and 4.3.1 of ICAO Doc 9880 Part IIB [5].

**[AMHS-LOG-A04]** All operator inputs shall be recorded and traceable for a configurable period (e.g. 30 days).

*Note: Section 5.9 of ICAO EUR Doc 020 [8] provides guidelines on the statistics to be produced for each MTA partner.*

#### A.2.1.7 Availability, Reliability, Maintainability

**[AMHS-ARM-A01]** A reliability, availability and maintainability analysis shall be conducted before entry into service and periodically thereafter to verify that AMHS End Systems satisfy or exceed the minimum requirements in these areas.

##### A.2.1.7.1 Availability

**[AMHS-ARM-A02]** An ATS Message Server and AFTN/AMHS Gateway shall be available 24 hours per day, with availability (defined as lack of unplanned outages) of at least 99.999% per year.

**[AMHS-ARM-A03]** An ATS Message User Agent shall be available as required, with availability of at least 99.99% per year.

**[AMHS-ARM-A04]** Precise constraints for the restart time are dependent on the configuration of the system and specific modes of failure, but for guidance a target restart time of less than 5 minutes shall be assumed.

**[AMHS-ARM-A05]** Components and system modes of failure which imply a restart time of more than 1 minute shall be identified.

**[AMHS-ARM-A06]** AMHS End Systems shall be designed such that processing of messages during recovery does not overload the system or degrade the performance below the performance targets.

#### A.2.1.7.2 Reliability

**[AMHS-ARM-A07]** AMHS End Systems shall be designed to minimise the effect of a failure of an AMHS End System or component thereof on the function of the entire system.

*Note: This requires an audit of design documentation to ensure that factors such as redundancy of components, alternative routings, etc. have been considered.*

**[AMHS-ARM-A08]** AMHS End Systems and their functional components shall be designed to avoid loss of messages.

#### A.2.1.7.3 Maintainability

**[AMHS-ARM-A09]** Commercial Off-the-Shelf (COTS), industry standard software, should be used as widely as possible, in order to enable an upward compatible growth path.

*Note: Refer to EUROCAE Document ED-109 [31] Section 4.1 for the applicability of software assurance level to COTS software.*

**[AMHS-ARM-A10]** AMHS End System implementations should be modular in nature and by using a series of industry standard interfaces provide a flexible and expandable combination of communication services.

### A.2.1.8 System Operation and Management

*Note: An ATS Messaging Management Centre (AMC) will continue to operate as a Common Facility for the benefit of the whole European area, to manage AMHS routing during the transition from AFTN/CIDIN to AMHS.*

#### A.2.1.8.1 Fault Management

**[AMHS-MGT-A01]** AMHS End System implementations shall support fault management in all components.

**[AMHS-MGT-A02]** It should be possible to schedule the execution of diagnostic tests.

**[AMHS-MGT-A03]** On detection of a fault condition, depending upon the fault severity and classification, AMHS End Systems should be configurable to perform one or more of the following actions, in increasing order of severity:

- a) Reconfigure;
- b) Switch over or re-assign resources;
- c) Perform software re-initialisation;
- d) Perform hardware re-initialisation.

**[AMHS-MGT-A04]** All fault conditions and actions shall be logged and remain accessible for a configurable period of not less than 1 month.

**[AMHS-MGT-A05]** The maximum period for stored events shall not be limited by the system design, and only be constrained by management configuration or the available resources of the specific system.

**[AMHS-MGT-A06]** An AMHS End System shall be able to meet its performance requirements when generation and storage of additional information (tracing) in support of basic failure analysis is enabled.

#### A.2.1.8.2 Configuration Management

**[AMHS-MGT-A07]** AMHS End Systems shall support the configuration management of all components.

**[AMHS-MGT-A08]** Where applicable, the AMHS End System or specific component should allow the on-line modification and activation of configuration parameters without requiring an interruption of service.

**[AMHS-MGT-A09]** The configuration, maintenance and activation of new addressing and routing information shall be possible through on-line modification without stopping the AMHS End System or substantially impairing its performance.

**[AMHS-MGT-A10]** The design of an AMHS End System shall not constrain the size of the address space or addressing and routing tables; these are only constrained by system management configuration or available system resources.

**[AMHS-MGT-A11]** All modifications of the application configuration should be logged.

**[AMHS-MGT-A12]** AMHS End Systems should have the capability to import data specified in the address management function of ICAO EUR Doc 021 [9].

#### A.2.1.8.3 Accounting Management

*Note: Accounting management requires usage information to be stored and maintained in a suitable format to enable it to be processed off-line to attribute resource usage to the individual users for accounting purposes, financial or otherwise. No specific requirements have been identified in this area.*

#### A.2.1.8.4 Performance Management

**[AMHS-MGT-A13]** AMHS End System implementations shall support the collection and analysis of performance management data.

**[AMHS-MGT-A14]** It should be possible for the collection of statistical data to be configured, including the use of filters and the specification of collection and consolidation intervals.

**[AMHS-MGT-A16]** ATS Message Server implementations shall export statistics data in accordance with the format specified in ICAO EUR Doc 021 [9], Appendix C.

**[AMHS-MGT-A17]** It should be possible to configure trigger conditions to automatically regulate and prevent processor or storage overloads.

**[AMHS-MGT-A18]** Statistics shall be provided for overall performance, use of overall capacity, use of component capacity, overall availability and component availability.

**[AMHS-MGT-A19]** Statistical data shall be stored and accessible for a configurable period of not less than 1 month.

#### A.2.1.8.5 Security Management

**[AMHS-MGT-A20]** AMHS End System implementations shall support security management functions, including management of access control lists, local user authentication and authorisation, in accordance with ICAO EUR AFS Security Guidelines [10].

*Note: In the Basic ATSMHS, these are locally managed functions independent of any technical features inherent to the AMHS.*

**[AMHS-MGT-A21]** Access control mechanisms shall be provided to restrict access to system management information.

**[AMHS-MGT-A22]** User roles with configurable access rights should be supported.

*Note: Examples of the roles and corresponding access rights that could be accommodated include:*

- *Traffic Management: corrective actions, message processing, on-line modification of routing;*
- *Technical Operation: all network management functions without modification of routing;*
- *Supervisor: all.*

#### A.2.1.8.6 System Monitoring Functions

**[AMHS-MGT-A23]** All events, occurring due to automatically triggered changes to the AMHS End System configuration, components or subscribers as well as occurring due to forced changes shall be indicated on-line (e.g. as system messages).

#### A.2.1.8.7 System Management Interface

**[AMHS-MGT-A24]** AMHS End System implementations shall include a systems management interface consistent with the provisions of ICAO EUR Doc 020 [8], with suitable access control.

**[AMHS-MGT-A25]** Communication between the management interface and the system should be through the use of an SNMP [40] compatible interface, enabling interoperability between manager and agent components (see ICAO EUR Doc 020 [8], section 5.8.5).

*Note: SNMP management information bases have been developed for monitoring X.400 systems, e.g. RFC 2789 [47]. These can be used by COTS monitoring products.*

#### A.2.1.9 Transitional Procedures

**[AMHS-MGT-A26]** Procedures for the introduction of ATSMHS into an international COM Centre shall be as specified in Appendix A of ICAO EUR Doc 021, ATS Messaging Management Manual [9].

### A.2.2 ATS Message Server Requirements

*Note: An ATS Message Server supporting the Basic ATSMHS includes an MTA and optionally one or more MSs, as specified in ICAO Doc 9880 Part IIB [5] sections 3.2.2 to 3.2.4.*

**[AMHS-AMS-A01]** An ATS Message Server shall route, store and forward ATS Messages, taking into account the applicable performance requirements and routing configuration.

**[AMHS-AMS-A02]** An ATS Message Server shall be able to support the routing of messages according to a non-hierarchical addressing plan, as well as the MF-Addressing Schemes specified in ICAO Doc 9880 Part IIB [5] section 2.5.1.4.

**[AMHS-AMS-A03]** An ATS Message Server should have the capability to import data specified in the routing management function of ICAO EUR Doc 021 [9].

**[AMHS-AMS-A04]** MTAs shall implement the P1 MTS transfer profile as specified in Appendix B Annex F of ICAO EUR Doc 020 [8] (profile AMH11 plus AMHS-specific features), for communication with other ATS Message Servers.

**[AMHS-AMS-A05]** MTAs shall implement the P1 IPM requirements profile as specified in Appendix B Annex B of ICAO EUR Doc 020 [8] (profile AMH22 plus AMHS-specific features), for IPM communication with other ATS Message Servers.

**[AMHS-AMS-A06]** MTAs shall support a P1 message length of at least 2 MByte.

**[AMHS-AMS-A07]** The ATS Message Server should support a common and standardised interface for the submission and delivery of messages.

**[AMHS-AMS-A08]** In support of the integration of an ATS Message User Agent into other computer applications, an API for the submission and delivery of messages using Open Group API specifications [38] may be specified.

*Note 1: The logical architecture includes an "AMHS User" and a "Local Application" for constructing and submitting messages, and for receiving messages from remote users. The Local Application is undefined, but a well-defined interface is provided for message submission and delivery.*

*Note 2: The above requirement supports the SES requirement for modularity of systems.*

**[AMHS-AMS-A09]** MTAs shall support the Distribution List (DL) functional group.

*Note: The DL+ER (Exempted Recipients) class of the DL functional group is outside the scope of this EUROCONTROL Specification. It may be supported according to local requirements.*

**[AMHS-AMS-A10]** It is recommended that the ATS Message Server should have the capability to open multiple associations between each pair of communicating MTAs (see ICAO EUR Doc 020 [8] section 5.2.2).

*Note: This means that there is no guarantee that messages are transferred in their received order, only that the start of transfer is independent of message size.*

**[AMHS-AMS-A11]** The ATS Message Server shall use the Monologue dialogue-mode of the Reliable Transfer Service Element (RTSE) protocol for associations between each pair of communicating MTAs.

#### A.2.2.1 EATMN Boundary Requirements

**[AMHS-AMS-A12]** EATMN boundary ATS Message Servers shall additionally have the capability to communicate with ATS Message Servers external to the EATMN, subject to bilateral agreement.

*Note: Communication with ATS Message Servers situated in countries external to the EATMN may use any appropriate solution, for example using the connection mode transport service of either the ATN/IPS (TCP/IP) or the ATN/OSI (TP4/CLNP), as defined in ICAO Annex 10, Volume III, Part 1 [26].*

### A.2.3 ATS Message User Agent Requirements

*Note 1: In the AMHS architecture defined in ICAO Doc 9880 Part IIB [5], each direct AMHS user is provided with an ATS Message User Agent to access the message transfer service. ATS Message User Agents include a UA to perform submission of messages to the message transfer service and delivery of messages from the message transfer service.*

*Note 2: The logical architecture includes an optional AMHS Message Store component for storing, on behalf of local direct AMHS users, messages received from other users as well as other information objects such as reports.*

*Note 3: The ATSMHS uses the Inter-Personal Messaging (IPM) protocol P2 for communication between UAs. ICAO Doc 9880 Part IIB [5] specifies the relevant IPM Content Type profile.*

*Note 4: In the Basic ATSMHS, each IPM message contains a single ia5-text or general-text body part.*

**[AMHS-AMU-A01]** ATS Message User Agents shall comply with the requirements specified in section 3.1 of ICAO Doc 9880 Part IIB [5] for the support of the Basic ATSMHS, summarised as the following requirements:

- A UA profile based on AMH21 as specified in ISO/IEC ISP 12062-2 [20];
- The requirements of Repertoire Group A, for messages including a body part whose type is an Extended Body Part Type of general-text-body-part type;
- Provisions related to traffic logging.

**[AMHS-AMU-A02]** It is recommended that standard ISO/IEC 10021 [18] protocols P3 and/or P7 should be used for message submission and delivery.

*Note: In the Basic ATSMHS, a UA can communicate with the MTS using P3, P7 or proprietary access protocols, as an implementation choice local to the AMHS MD. The above recommendation is intended to foster seamless operation and enable a smooth transition to the Extended ATSMHS.*

**[AMHS-AMU-A03]** The maximum message-text length supported by the UA shall be a configurable parameter value.

**[AMHS-AMU-A04]** A UA shall be capable of accepting and processing a maximum received message-text length of at least 64 kByte and be capable of handling messages longer than the maximum length without malfunction.

*Note: ICAO EUR Doc 020 [8] section 5.2.1 recommends support of AFTN messages up to 64 kByte. It is a local implementation matter how to handle received messages longer than the maximum supported message length.*

**[AMHS-AMU-A05]** If a user application is co-located with an MTA on a common platform, then the interface between the application's (logical) UA and the message transfer service shall provide equivalent functionality to the MT-Access abstract service as defined for the P3 access protocol specified in ISO/IEC 10021-6 [18].

*Note: Some Message Server configurations may include a co-located UA or Access Unit that provides access to remote users via protocols external to AMHS.*

**[AMHS-AMU-A06]** If "forced" delivery to a UA is required (e.g. for reception of urgent, high priority messages) then either the P3 protocol or (in the case of MS) P7 with Alerts configured should be used.

**[AMHS-AMU-A07]** It should be possible for direct AMHS users to request confirmation of delivery and to receive delivery reports.

## A.2.4 Message Store Requirements

*Note 1: The MS is Optional in the AMHS logical architecture. It is a local decision whether MS functionality is required. The local options of the MS that are appropriate to the MS user's intended task need to be specified when procuring an ATS Message Server.*

*Note 2: In ICAO EUR Doc 020 [8], there is no distinction between the MS and enhanced MS(94), since the enhancements in the MS(94) standards 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).*

**[AMHS-MST-A01]** It is recommended that, when an MS is included in the ATS Message Server, standard ISO/IEC 10021 [18] protocol P3 should be used between the MS and MTA for message submission and delivery.

*Note: In the Basic ATSMHS, an MS can communicate with the MTS using P3 or proprietary access protocols, as an implementation choice local to the AMHS MD. The above recommendation is intended to foster seamless operation and enable a smooth transition to the Extended ATSMHS.*

**[AMHS-MST-A02]** It is recommended that the standard ISO/IEC 10021 [18] protocol P7 should be used between MS and UA for message retrieval and indirect submission.

*Note: In the Basic ATSMHS, a UA can communicate with the MS using P7 or proprietary access protocols, as an implementation choice local to the AMHS MD. The above recommendation is intended to foster seamless operation and enable a smooth transition to the Extended ATSMHS.*

**[AMHS-MST-A03]** It is recommended that the MS application context should exclude the RTSE.

*Note: This differs from ICAO EUR Doc 020 [8] Appendix B, where the inclusion and use of RTSE is left Optional in the MS protocol stack; it is a local implementation decision whether or not RTSE is required for message submission and retrieval. The above recommendation is intended to foster a common approach using "lightweight" UA protocols over a robust network service.*

**[AMHS-MST-A04]** MS implementations may support the Distribution List (DL) functional group.

*Note: The DL Exempted Recipients class (DL+ER) is an Optional functional group in profiles AMH13 and AMH15. It is only needed if support of dl-exempted-recipients is required in the message submission envelope. DL is required by the P7 profile in Appendix B Annexes H and I of ICAO EUR Doc 020 [8].*

**[AMHS-MST-A05]** Requirements for the maximum number of MS users that can be simultaneously supported by an MS implementation shall be based upon current and foreseen ATSMHS usage.

## A.2.5 AFTN/AMHS Gateway Requirements

*Note: An AFTN/AMHS Gateway supporting the Basic ATSMHS includes an MTA and an Access Unit (the Message Transfer and Control Unit – MTCU), as specified in ICAO Doc 9880 Part IIB [5] chapter 4.*

**[AMHS-GWY-A01]** Where interworking with AFTN end systems is required, a gateway between the AMHS and AFTN message services shall be implemented in conformance with ICAO Doc 9880 Part IIB [5] chapter 4.



**[AMHS-GWY-A02]** An AFTN/AMHS Gateway supporting the Basic ATSMHS shall implement all elements which are applicable to the Basic ATSMHS and which are marked as “M” in the “ATS Messaging Service” column of ICAO Doc 9880 Part IIB Table 4-3.

**[AMHS-GWY-A03]** The AFTN/AMHS Gateway shall support address conversion of O/R addresses belonging to a non-hierarchical addressing plan, as well as the MF-Addressing Schemes specified in ICAO Doc 9880 Part IIB [5] section 2.5.1.4.

**[AMHS-GWY-A04]** The AFTN/AMHS Gateway shall support address conversion and routing for all currently assigned ICAO eight-letter addressee indicators (AF-addresses).

**[AMHS-GWY-A05]** The AFTN/AMHS Gateway should have the capability to import the address mapping tables in comma-separated value (CSV) format provided by the European ATS Messaging Management Centre (AMC).

*Note: In the ICAO Doc 9880 Part IIB [5] specification of the AFTN/AMHS Gateway, a small number of implementation details are left to the decision of Management Domains, i.e. of ANSPs implementing AMHS. The most significant of these elements is related to message splitting when leaving the AMHS, because of the increased message lengths that are allowed in the European AFTN in support of ADEXP. To achieve sufficient flexibility in support of these existing messaging requirements the following procedure is defined:*

**[AMHS-GWY-A06]** If the length of the ATS-Message-Text element in an AMHS message exceeds the maximum supported length (a parameter set initially to 64 kByte, in accordance with current AFTN/CIDIN practices for the support of ADEXP messages), the message shall be rejected by the AFTN/AMHS Gateway’s MTCU as specified in ICAO Doc 9880 Part IIB [5] section 4.5.2.1.7 a).

*Note: The above requirement originates from the SPACE project. It modifies the specification of the AFTN/AMHS gateway in ICAO Doc 9880 Part IIB [5], section 4.5.2.1.7, in that an upper limit is defined for the size of a message that can be converted. In ICAO Doc 9880 Part IIB, the message size is limited only by system resources.*

**[AMHS-GWY-A07]** If the length of the ATS-Message-Text element in an AMHS message exceeds 1800 characters but does not exceed the maximum supported length, the AFTN component of the AFTN/AMHS Gateway shall handle the message using one of the following options, depending on the AFTN/CIDIN capability of the next international COM centres towards the destination:

- a) Transfer the message without modification; or
- b) Truncate the message text to 1800 characters; or
- c) Perform the message splitting procedure specified in ICAO Doc 9880 Part IIB [5] section 4.5.2.1.7 b).

*Note: The above requirement originates from the SPACE project. It modifies the specification of the AFTN/AMHS gateway in ICAO Doc 9880 Part IIB [5], section 4.5.2.1.7, in that messages with text length between 1801 characters and the upper limit may be transferred without being split, or may be truncated. ICAO Doc 9880 Part IIB specifies only that the message is split “if the procedure proposed in Annex 10 Volume II Attachment B is applied in the AFTN/AMHS Gateway”. It does not alter in any way current AFTN/CIDIN practices.*

## A.3 CONFORMITY ASSESSMENT MATERIALS

This section includes the profile requirements list (PRL) for the communications services specified in Annex A.

### A.3.1 Compliance Statement

**[AMHS-CA-A01]** A claim of conformance for an implementation shall be supported by completion of the relevant Protocol Implementation Conformance Statement (PICS) pro forma.

**[AMHS-CA-A02]** Implementers claiming conformance to the specified services shall complete the PICS specified in Appendix B Annex Q of ICAO EUR Doc 020 [8].

*Note: For AMHS components except the AFTN/AMHS Gateway, the EUR AMHS profile specification in [8] contains a corresponding Implementation Conformance Statement (ICS) pro forma that is intended to document each implementation's conformance to the Base Standards, the referenced ISPs, the ICAO technical provisions and the corresponding EUR Profile Annexes.*

**[AMHS-CA-A03]** Implementers shall state whether all of the requirements and which of the optional elements of the AFTN/AMHS Gateway supporting the Basic ATSMHS as specified in ICAO Doc 9880 Part IIB [5] section 4 have been implemented, using the tables in this section, or equivalent.

*Note 1: The following legend is used in Table A-1*

M = Mandatory Support  
C.x = At least one must be supported  
O = Optional Support  
I = Out of Scope

*Note 2: FTBP, IHE, SEC and DIR functional groups are specified as Optional in ICAO Doc 9880 (Table 3-6) for ATS Message Server and ATS Message User Agent claiming Basic ATSMHS conformance. For an AFTN/AMHS Gateway, FTBP is not relevant; SEC could be applicable in the AMHS-to-AFTN direction but is not currently specified. IHE and DIR could optionally be supported.*

**Table A-1: Profile requirements list for AFTN/AMHS Gateway supporting the Basic ATSMHS**

PRL Ref Basic	Question/Feature	Doc 9880 Part IIB Ref	Profile Req	Supplier Response	Notes
	<b>Subsetting Rules</b>	<b>3.4</b>			
1	<b>Classification of ATSMHS Functional Groups</b>	<b>Table 3-6</b>			
	Which of the following functional groups are supported?				
1.1	Basic ATS Message Handling Service		M		Basic
1.2	Use of File Transfer Body Parts for Binary data exchange		N/A		FTBP
1.3	Use of IPM Heading Extensions		O		IHE
1.4	AMHS Security		I		SEC
1.5	Use of Directory		O		DIR

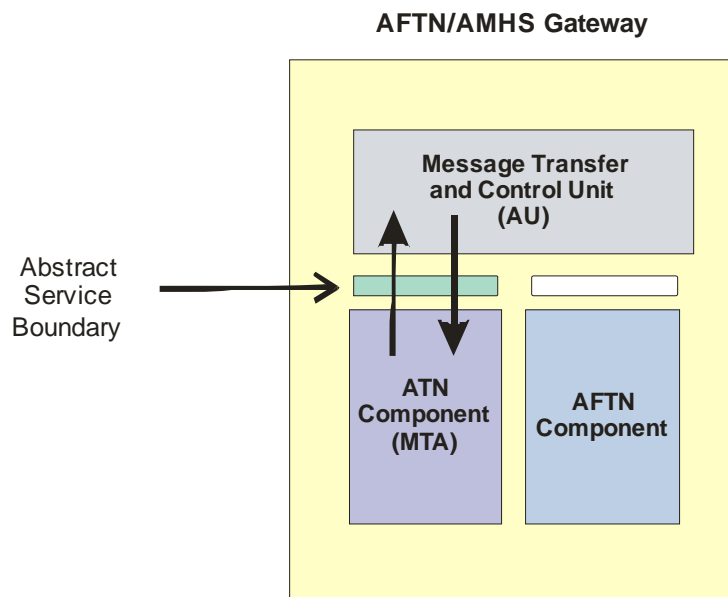
EUROCONTROL SPECIFICATION  
on the  
Air Traffic Services Message Handling System (AMHS)

PRL Ref Basic	Question/Feature	Doc 9880 Part IIB Ref	Profile Req	Supplier Response	Notes
	<b>Definition of ATSMHS subsets</b>	<b>Table 3-7</b>			
2	Which of the following subsets is supported?				
2.1	I. Basic ATS Message Handling Service (Basic)		M		
2.2	II. Basic + FTBP		I		Out of scope
2.3	III. Basic + IHE		I		Out of scope
2.4	IV. Basic + DIR		I		Out of scope
2.5	V. Basic + DIR + FTBP		I		Out of scope
2.6	VI. Basic + DIR + IHE		I		Out of scope
2.7	VII. Basic + DIR + SEC		I		Out of scope
2.8	VIII. Basic + IHE + DIR + SEC		I		Out of scope
2.9	IX. Basic + IHE + DIR + FTBP		I		Out of scope
2.10	X. Basic + IHE + DIR + FTBP + SEC		I		Out of scope
3	<b>Message Transfer and Control Unit</b>				
3.1	<b>Conversion of AFTN Acknowledgement Messages</b>	<b>4.4.3</b>			
3.1.1	Is the case of the user element of the IPM-identifier modified when constructing a RN?	4.4.3.3.3.1	O		
3.2	<b>AMHS IPM Conversion</b>	<b>4.5.2</b>			
3.2.1	Is conversion from ISO 8859-1 to IA5IRV supported?	4.5.2.1.4 a) 4)	O		
3.2.1.2	Can the conversion be modified to support locally defined conversion rules?		O		
3.2.2	If recipient names cannot be translated into an AF-Address how many non-delivery reports are generated?	4.5.2.2.6.2.1			
3.2.2.1	One report for each failure		C.a		
3.2.2.2	A single report		C.a		
3.2.4	<b>For ATS-Message-Text length &gt;1800 characters:</b>		-		
3.2.4.1	Is the maximum ATS-Message-Text length limited by parameter setting?		M		
3.2.4.1.1	What is the range of values for the maximum message length parameter?		-		Default 64 kB
3.2.4.2	Can a "long" AFTN message of the same length be generated by the MTCU?		C.b		
3.2.4.3	Can an AFTN message truncated to 1800 characters be generated by the MTCU?		C.b		
3.2.4.4	Is the message splitting procedure in Annex 10 Volume II Attachment B supported?		C.b		
3.3	<b>Generation of AMHS reports</b>	<b>4.5.6</b>			

EUROCONTROL SPECIFICATION  
on the  
Air Traffic Services Message Handling System (AMHS)

PRL Ref Basic	Question/Feature	Doc 9880 Part IIB Ref	Profile Req	Supplier Response	Notes
3.3.1	Is a single non-delivery report generated on the rejection for multiple recipients?	4.5.6.1.2	O		
3.3.2	Is a single delivery report generated for multiple recipients?	4.5.6.1.4	O		
3.3.3	Is the case of the <i>global-domain-identifier</i> element of the <i>MTS-identifier</i> modified when constructing a report?	4.5.6.2.11.1	O		
3.3.4	Is the Return Of Content (RoC) Functional Group implemented in the MTCU?	4.5.6.2.16.1	O		

*Note: ICAO Doc 9880 Part IIB expresses the functional requirements of the AFTN/AMHS Gateway component using tabular profile requirement lists which apply at the abstract service boundary between the ATN Component (MTA) and the MTCU of the AFTN/AMHS Gateway, as shown in Figure A-1.*



**Figure A-1: MTCU and ATN Component Abstract Service Boundary**

**[AMHS-CA-A04]** For AFTN/AMHS Gateway implementations, a PICS shall be provided stating the level of support, for each of the elements relevant to support of the Basic ATSMHS, listed in the profile requirements lists in section 4 of ICAO Doc 9880 Part IIB [5] and specified in Table A-2.

**Table A-2: MTCU Profile Requirements for the Basic ATSMHS**

Reference ICAO Doc Part IIB	in 9880	Description
Table 4-3		Specifies the required and optional elements for the generation of an IPM when converting a received AFTN message to AMHS. The column headed "ATS Mess. Service" in the referenced Table specifies the static capability requirements of an IPM AU supporting the ATSMHS. Elements marked with an asterisk (*) are not applicable and elements marked as "C1" are optional for AFTN/AMHS Gateway implementations supporting the Basic ATSMHS level of service.
Table 4-4		Specifies the required and optional elements for the generation of a message transfer envelope when converting from AFTN to AMHS. The column headed "ATS Mess. Service" in the referenced Table specifies the static capability requirements of an IPM AU supporting the ATSMHS. Elements marked with an asterisk (*) are not applicable for AFTN/AMHS Gateway implementations supporting the Basic ATSMHS level of service.
Table 4-6		Specifies the required and optional elements for the generation of an AMHS Receipt Notification resulting from the receipt of an AFTN acknowledgement message. The column headed "Basic ATS Mess. Service" in the referenced Table specifies the static capability requirements of an IPM AU supporting the Basic ATSMHS.
Table 4-7		Specifies the required elements for the generation of a message transfer envelope for an AMHS Receipt Notification resulting from the receipt of an AFTN acknowledgement message. The column headed "Basic ATS Mess. Service" in the referenced Table specifies the static capability requirements of an IPM AU supporting the Basic ATSMHS.
Table 4-9		Specifies the required and optional elements for the generation of an AFTN message when converting from AMHS. The column headed "ATS Mess. Service" in the referenced Table specifies the static capability requirements of an IPM AU supporting the ATSMHS. Elements marked with an asterisk (*) are not applicable for AFTN/AMHS Gateway implementations supporting the Basic ATSMHS level of service.
Table 4-10		Specifies the required support of elements in a received message transfer envelope when converting from AMHS to AFTN. The column headed "ATS Mess. Service" in the referenced Table specifies the static capability requirements of an AU in relation to the message transfer elements of service.
Table 4-12		Specifies the required support of elements in a received AMHS Receipt Notification when converting to an AFTN acknowledgement message. The column headed "Basic ATS Mess. Service" in the referenced Table specifies the static capability requirements of an IPM AU supporting the Basic ATSMHS.
Table 4-13		Specifies the required support of elements in a message transfer envelope received with an AMHS Receipt Notification when converting to AFTN. The column headed "Basic ATS Mess. Service" in the referenced Table specifies the static capability requirements of an AU in relation to the message transfer elements of service.
Table 4-15		Specifies the required support of elements in a received AMHS Report when converting to an AFTN service message. The column headed "Basic ATS Mess. Service" in the referenced Table specifies the static capability requirements of an IPM AU supporting the Basic ATSMHS.

Reference in ICAO Doc 9880 Part IIB	Description
Table 4-16	Specifies the required support of elements when generating an AMHS Report. The column headed "Basic ATS Mess. Service" in the referenced Table specifies the static capability requirements of an AU supporting the Basic ATSMHS.

### A.3.2 Testing Requirements

**[AMHS-CA-A05]** AMHS End Systems shall be tested according to suitable test cases and procedures ensuring adequate coverage of the BASIC functional group.

*Note: Suitable test cases are specified in Appendices C to F of ICAO EUR Doc 020 [8].*

**[AMHS-CA-A06]** Testing shall be conducted within a common framework consistent with the procedures in ICAO EUR Doc 020 [8] using appropriate test tools and procedures.

*Note 1: As part of the assessment of the conformity or suitability for use of constituents required by the interoperability Regulation, the manufacturer is responsible for: determining the appropriate test environment, verifying that there exists a test plan providing full coverage of applicable requirements, ensuring the consistency and quality of the technical documentation and the test plan, performing the inspections and tests as specified in the test plan and writing the report presenting the results of inspections and tests.*

*Note 2: As part of the verification of systems required by the interoperability Regulation, the ANSP or Notified Body is responsible for: verifying that there exists a test plan providing full coverage of the interoperability and performance requirements, ensuring the consistency and quality of the technical documentation and the test plan, performing the inspections and tests as specified in the test plan and writing the report presenting the results of inspections and tests.*

**EUROCONTROL SPECIFICATION**  
**on the**  
**Air Traffic Services Message**  
**Handling System (AMHS)**  
**ANNEX B – Extended Service**

**SPECIFICATION DOCUMENT IDENTIFIER: EUROCONTROL-SPEC-0136**

<b>Edition Number</b>	<b>:</b>	<b>2.0</b>
<b>Edition Date</b>	<b>:</b>	<b>18/09/2009</b>
<b>Status</b>	<b>:</b>	<b>Released</b>
<b>Intended for</b>	<b>:</b>	<b>General Public</b>
<b>Category</b>	<b>:</b>	<b>EUROCONTROL Specification</b>

## DOCUMENT CHANGE RECORD

The following table records the complete history of the successive editions of the present document.

EDITION NUMBER	EDITION DATE	INFOCENTRE REFERENCE	REASON FOR CHANGE	PAGES AFFECTED
0.6	24/10/08		Created after informal stakeholder review from split of previous Annex A into 2 parts – Basic & Extended ATSMHS	All
1.0	08/12/08		Updated after informal stakeholder review. Input to formal consultation.	All
1.1	27/07/09		Updated after ENPRM-09/001 formal consultation.	All
2.0	18/09/09		Released Issue	Footers



## CONTENTS

<b>ANNEX B - SPECIFICATION OF EXTENDED INTEROPERABILITY REQUIREMENTS .....</b>	<b>1</b>
B.1 CONFIGURATION CONTROL .....	1
B.2 REQUIREMENTS AND EXPLANATORY MATERIALS .....	2
B.2.1 Common Requirements .....	2
B.2.1.1 Standards Baseline .....	2
B.2.1.2 General Requirements .....	3
B.2.1.3 Naming and Addressing .....	3
B.2.1.4 Safety Requirements .....	3
B.2.1.5 Performance Requirements .....	3
B.2.2 ATS Message Server Requirements .....	3
B.2.2.1 General .....	3
B.2.2.2 P1 Message Transfer .....	4
B.2.2.3 P3 Message Access .....	4
B.2.2.4 Directory Access .....	5
B.2.3 ATS Message User Agent Requirements .....	5
B.2.3.1 General .....	5
B.2.3.2 IPM Content .....	6
B.2.3.3 P3 Access .....	7
B.2.3.4 P7 Access .....	8
B.2.3.5 Directory Access .....	8
B.2.4 Message Store Requirements .....	9
B.2.4.1 General .....	9
B.2.4.2 MS Access to MTA .....	9
B.2.4.3 P7 Access .....	10
B.2.5 AFTN/AMHS Gateway Requirements .....	10
B.2.5.1 General .....	10
B.2.5.2 Directory Access .....	10
B.3 CONFORMITY ASSESSMENT MATERIALS .....	12
B.3.1 Compliance Statement .....	12
B.3.2 Testing Requirements .....	16



## ANNEX B – SPECIFICATION OF AMHS EXTENDED INTEROPERABILITY REQUIREMENTS

### B.1 CONFIGURATION CONTROL

#### B.1.1 MOC ELEMENT IDENTIFICATION

MOC_Title	MOC_Version	MOC_Edition
AMHS_EXT_IOP	1	1

#### B.1.2 MOC ELEMENT CHANGE RECORD

The following table records the complete history of the successive editions of MOC specifications.

Version Number	Edition Number	Edition Date	Reason for Change	Sections Affected
1	1	18/09/09	Initial specification	All

#### B.1.3 MOC ELEMENT TRACEABILITY TOWARDS REGULATORY PROVISIONS

The following table records the traceability history of regulatory provisions associated with this MOC element.

Version Number	Edition Number	Implementing rule references	References of regulatory provisions	Validation date
1	1	N/A	Regulation (EC) No 552/2004 [1] Annex II Part A and Part B (4) - Essential requirements applicable to communications systems and procedures for ground-to-ground communications	

#### B.1.4 MOC ELEMENT TRACEABILITY TOWARDS INTERNATIONAL STANDARDS

The following table records the traceability of international standards associated with this MOC element.

International standards identification	References of text parts used to derive MOC specifications	Standards text incorporated by reference into the MOC element
ICAO Doc 9880 Part IIB [5]	(Extended ATSMHS)	
ICAO EUR Doc 020 [8]		Appendix B

## B.2 REQUIREMENTS AND EXPLANATORY MATERIALS

*Note 1: This normative Annex is an integral part of this EUROCONTROL Specification. It specifies requirements for AMHS End Systems that support the Extended ATSMHS as defined in ICAO Doc 9880 Part IIB [5].*

*Note 2: This Annex must be read in conjunction with the Main Body of this EUROCONTROL Specification, which provides definitions, document references and contextual information. References given in square brackets are defined in section 10 of the Main Body. Reference is also made to Annex A of this EUROCONTROL Specification for the definition of the Basic ATSMHS, and to Annex C for DUA details.*

*Note 3: The Extended ATSMHS is functionally a superset of the Basic ATSMHS, and is backward compatible with it, in that the ability to downgrade to the Basic ATSMHS level of service is required. AMHS End Systems claiming compliance with the requirements in this Annex must also be compliant with the requirements in Annex A.*

*Note 4: The Extended ATSMHS satisfies the SES essential requirement to support new concepts of operation by providing for the general exchange of binary data or files and, if the AMHS SEC functional group is implemented, enabling strong authentication and data integrity services between peer direct AMHS users. (Note that the use of AMHS Security is not included, nor needed for compliance with this Annex). Seamless operation between a direct AMHS user and an ATS Message Server is achieved through the specification of a standard profile for the access protocol. Further, the Extended ATSMHS benefits from a standardised directory function, which can be used to enhance seamless operation by ensuring the up-to-date dissemination of address and configuration information.*

*Note 5: This Annex is structured such that requirements common to all AMHS End Systems supporting the Extended ATSMHS are specified in section B.2.1, followed by requirements specific to each AMHS End System type. Compliance is conditional upon the type of AMHS End System under consideration (e.g. section B.2.2 on ATS Message Server is not applicable when considering requirements for ATS Message User Agents).*

### B.2.1 Common Requirements

#### B.2.1.1 Standards Baseline

**[AMHS-BAS-B01]** AMHS End Systems shall comply with the standards identified in Annex A of this EUROCONTROL Specification unless stated otherwise.

**[AMHS-BAS-B02]** AMHS End Systems conforming to this Annex shall comply with the requirements specified in ICAO Doc 9880 Part IIB [5], including those requirements specific to the support of the Extended ATSMHS, unless explicitly stated otherwise in this Annex.

**[AMHS-BAS-B03]** In the event of conflicting requirements not explicitly identified, the specification in ICAO Doc 9880 Part IIB [5] shall take precedence.

*Note: ICAO Doc 9880 Part IIB [5] paragraph 2.2.4.1.b) requires the storage of management information about ATS Message Servers and AFTN/AMHS Gateways in the ATN cross-domain management information base (XMIB). This is not required for conformance to this EUROCONTROL Specification.*

### B.2.1.2 General Requirements

**[AMHS-GEN-B01]** ATS Message Servers and ATS Message User Agents shall conform to configuration IX as defined in ICAO Doc 9880 Part IIB [5] section 3.4 (i.e. functional groups Basic + IHE + DIR + FTBP).

*Note: Migration to configuration X (addition of AMHS functional group SEC) may be foreseen at some time in the future, but is not currently required for compliance with this EUROCONTROL Specification.*

**[AMHS-GEN-B02]** AMHS End Systems shall support the object classes and attribute types of directory information specified in ICAO EUR Doc 020 [8] Appendix B Annex K.

**[AMHS-GEN-B03]** AMHS End Systems shall support the implementation of advanced, agreed and validated concepts of operation by providing managed access to the messaging system for new end-user applications via well-defined interfaces.

*Note: The basic recommendation for the use of standardised interfaces wherever possible also applies to AMHS components supporting the Extended ATSMHS. However, it is noted that the Open Group APIs are not fully compliant with extended service requirements such as support for the Business Class (BC) functional group, so some customisation may be necessary.*

### B.2.1.3 Naming and Addressing

**[AMHS-N&A-B01]** The responsible operators of AMHS Management Domains shall register a unique directory name for each AMHS user in their domain.

### B.2.1.4 Safety Requirements

*Note: There are no additional safety requirements specified in this Annex. The safety requirements specified in Annex A are fully applicable to elements of the Extended ATSMHS.*

### B.2.1.5 Performance Requirements

*Note: There are no additional performance requirements specified in this Annex. The performance requirements specified in Annex A are fully applicable to elements of the Extended ATSMHS. However, it should be noted that the use of binary attachments will tend to result in larger message sizes. Unless the number of messages with file transfer body parts is very small, there will be an impact on performance. Also, the use of security will increase the submission time and also the time to open a message.*

## B.2.2 ATS Message Server Requirements

### B.2.2.1 General

*Note: An ATS Message Server supporting the Extended ATSMHS includes an MTA, a DUA and optionally one or more MSs, as specified in ICAO Doc 9880 Part IIB [5] sections 3.2.2 to 3.2.5.*

### B.2.2.2 P1 Message Transfer

**[AMHS-AMS-B01]** MTAs shall implement the P1 MTS transfer profile AMH11 as specified in Annex A of this EUROCONTROL Specification, with the addition of support of the DIR Functional Group as specified in ICAO Doc 9880 Part IIB [5], section 3.2.4.2.

**[AMHS-AMS-B02]** MTAs should implement the SEC Functional Group of the P1 IPM requirements profile AMH22, for security class S0, in addition to the AMH22 requirements specified in Annex A of this EUROCONTROL Specification.

*Note 1: The above recommendation differs from ICAO Doc 9880 Part IIB, which does not explicitly state support for the SEC FG in profiles AMH11 and AMH22, but implicitly mandates such support for the Extended ATSMHS. MTA support of the SEC functional group for P1 is specified as Optional for the EUR AMHS Profile in Appendix B Annex B (AMH22) and Annex F (AMH11) of ICAO EUR Doc 020 [8].*

*Note 2: Implementation of the SEC Functional Group of profile AMH22 also implies implementation of the SEC Functional Group of profile AMH11; AMH22 does not add any IPM-specific requirements.*

*Note 3: Support of the SEC(S0) FG of profile AMH11 means that MTAs support and use initiator-credentials and responder-credentials fields in the MTABind operation for simple authentication (strong authentication may optionally be bilaterally agreed). It means support (but not necessarily use) of the Message Token extension data type, including the signed-data element.*

### B.2.2.3 P3 Message Access

**[AMHS-AMS-B03]** MTAs supporting direct message submission and delivery shall support P3 access conforming to the profile in Appendix B Annex G of ICAO EUR Doc 020 [8].

*Note: The referenced profile requires conformance to MHS Profile AMH12 and optionally also allows support of MHS Profile AMH14. It requires support of the DL functional group and the file transfer encoded information type.*

**[AMHS-AMS-B04]** MTAs supporting direct message submission and delivery shall support IPM P3 access conforming to the profile in Appendix B Annex C of ICAO EUR Doc 020 [8], with the addition of support of the DIR Functional Group as specified in ICAO Doc 9880 Part IIB [5], section 3.1.4.3.1.

*Note: The referenced profile requires conformance to MHS Profiles AMH23 and AMH25. It requires support of the DL functional group.*

**[AMHS-AMS-B05]** MTAs should additionally implement the SEC Functional Group of the IPM P3 Access profile AMH23/AMH25, for security class S0.

*Note 1: The above recommendation, if followed, enables authentication between MTAs and their users and provides forward compatibility for secure messaging. ICAO Doc 9880 Part IIB states that SEC(S0) support is required for the Extended ATSMHS, but also implies that such support is conditional upon the ATSMHS SEC functional group. MTA support of the SEC functional group for P3 is specified as optional for the EUR AMHS Profile in Appendix B Annex C (AMH23/AMH25) and Annex G (AMH12/AMH14) of ICAO EUR Doc 020 [8].*

*Note 2: Implementation of the SEC Functional Group of profile AMH23/AMH25 also implies implementation of the SEC Functional Group of profile AMH12/AMH14, with the addition of support for certificates in the IPM message submission and delivery envelopes.*

*Note 3: Implementation of the SEC(S0) FG of profile AMH12/AMH14 means that MTAs support and use initiator-credentials and responder-credentials fields in the MTSBind*

operation for simple authentication (strong authentication may optionally be bilaterally agreed). It also means support (but not necessarily use) of the *SubmissionControl* element and the *Message Token* extension data type, including the signed-data element. Security related fields in submission and delivery envelopes are minimally supported, i.e. relayed transparently between MTA and MTS-user.

#### B.2.2.4 Directory Access

**[AMHS-AMS-B06]** An ATS Message Server implementing the DIR functional group shall include a DUA for access to the ATN Directory.

*Note 1: Annex C of this EUROCONTROL Specification specifies DUA requirements.*

*Note 2: ISO/IEC ISP 10611-1 [19] notes that an MTA may access a directory service using a DUA. The interface between the MTA and the DUA is a local matter. The minimum information that is required to be capable of being returned by the directory service is an attribute containing one or more OR-addresses. A supplementary class of the DIR Functional Group, DIR+SEC adds the requirement for the User Certificates and Supported Algorithms attributes, and the Certificate Match matching-rule. The use of a directory service to support distribution list processing is defined in the DL+DIR class of the DL FG, and requires support for the MHS Distribution List object-class and for the MHS DL Members, MHS DL Policy and MHS DL Submit Permissions attributes. Support of the supplementary class DIR+ROUT to support MHS Routing is not required for AMHS implementation.*

### B.2.3 ATS Message User Agent Requirements

#### B.2.3.1 General

*Note 1: An ATS Message User Agent supporting the Extended ATSMHS includes an IPM UA and a DUA, as specified in ICAO Doc 9880 Part IIB [5] sections 3.1.2 to 3.1.5.*

*Note 2: The UA in the Extended ATSMHS supports the P3 protocol to access the MTA in an ATS Message Server and/or the P7 protocol to access the MS in an ATS Message Server, where available.*

*Note 3: In the Extended ATSMHS, each IPM message may contain a combination of ia5text, general text and file transfer body parts. Use of the Bilaterally Defined body part type is prohibited for sending, though it must be supported for reception for backwards compatibility – see ICAO Doc 9880 Part IIB [5] paragraph 3.1.4.2.1.2.*

**[AMHS-AMU-B01]** An ATS Message User Agent supporting the Extended ATSMHS shall comply with the requirements specified in section 3.1 of ICAO Doc 9880 Part IIB [5] for the support of the Extended ATSMHS, summarised as the following requirements;

- A UA profile based on Profile AMH21 as specified in ISO/IEC ISP 12062-2 [20];
- The requirements of Repertoire Group A, for messages including a body part whose type is an Extended Body Part Type of general-text-body-part type;
- Support of the IPM Business Class (BC) functional group as specified in ISO/IEC ISP 12062-2 [20]
- Support of the file-transfer body part;
- UA access profile based on Profiles AMH23 or AMH25 for P3 access to the MTS, or based on Profiles AMH24 or AMH26 for P7 access to the MS, as specified in ISO/IEC ISP 12062 [20] parts 4, 5 and 6;

- The additional provisions relating to parameters generated at an ATS Message User Agent, as specified for the Extended ATSMHS;
- Provisions related to traffic logging.
- A DUA profile supporting the defined access profile and the specified object classes and attribute types.

### B.2.3.2 IPM Content

**[AMHS-AMU-B02]** A UA in an ATS Message User Agent supporting the Extended ATSMHS shall conform to the profile in Appendix B Annex A of ICAO EUR Doc 020 [8].

*Note: The referenced profile requires conformance to MHS Profile AMH21. It requires support of the file transfer encoded information type.*

**[AMHS-AMU-B03]** A UA in an ATS Message User Agent shall be prohibited from sending messages containing a Bilaterally Defined body part.

**[AMHS-AMU-B04]** A UA shall additionally implement the elements of the BC Functional Group of the IPM Content profile AMH21 indicated as “m” in the “Support” column of Table B-1, as specified in ICAO Doc 9880 Part IIB [5], section 3.1.4.2.1.

*Note 1: This requirement differs from Appendix B Annex A of ICAO EUR Doc 020 [8], where UA support of the BC functional group is specified as Optional.*

*Note 2: The support requirements for the BC functional group are indicated in the following table, which modifies the requirements of profile AMH21 in ISO/IEC ISP 12062-2 [20], paragraph A.2.5 and extends Table 3-2 in ICAO Doc 9880 Part IIB [5]. Elements indicated as “o” in the “Support” column of Table B-1 are not required for AMHS.*

*Note 3: A sending UA needs to ensure that all message recipients also support the BC functional group. This could be achieved by Directory lookup.*

**[AMHS-AMU-B05]** The values of the *precedence* field in the per-recipient heading fields of a message shall be the same for all recipients, as this field corresponds to AFTN Priority.

**Table B-1: IPM Business Class (BC) support requirements**

#### IPM heading fields

Ref	Element	ISP		Support	
		Orig.	Rec.	Orig.	Rec.
17.6	authorization-time	m	m	m	m
17.7	circulation-list-recipients	m	m	o	o
17.8	distribution-codes	m	m	o	o
17.10	information-category	m	m	o	o
17.11	manual-handling-instructions	m	m	o	o
17.12	originators-reference	m	m	m	m
17.13	precedence-policy-identifier	m	m	m	m

#### Common data types

Ref	Element	ISP		Support	
		Orig.	Rec.	Orig.	Rec.
A.1.5/1.4.2	circulation-list-indicator		m		o
A.1.5/1.4.3	precedence	m	m	m	m



*Note: UA support of the IPM Security (SEC) functional group is also specified as Optional in Appendix B Annex A of ICAO EUR Doc 020 [8]. However, support of IPM-specific security features SEC-n is not required, nor is it specified in ICAO Doc 9880 Part IIB. Instead, any security functionality is provided by the Common Messaging security class S0; there are no additional requirements for a UA in an IPM environment.*

### B.2.3.3 P3 Access

**[AMHS-AMU-B06]** A UA supporting P3 access shall conform to the profile in Appendix B Annex G of ICAO EUR Doc 020 [8].

*Note: The referenced profile requires conformance to MHS Profile AMH12 and optionally also allows support of MHS Profile AMH14. It requires support of the DL functional group and the file transfer encoded information type.*

**[AMHS-AMU-B07]** A UA supporting P3 access shall conform to the profile in Appendix B Annex C of ICAO EUR Doc 020 [8], with the addition of support of the DIR Functional Group as specified in ICAO Doc 9880 Part IIB [5], section 3.1.4.3.1.

*Note 1: The referenced profile requires conformance to MHS Profiles AMH23 and/or AMH25. It requires support of the DL functional group.*

*Note 2: Unlike the P7 Access profiles AMH24/AMH26, the P3 Access profiles AMH23/AMH25 do not specify a BC Functional Group. Instead, the optional BC Functional Group is inherited from the IPM Content profile AMH21, as specified above.*

**[AMHS-AMU-B08]** It is recommended that a UA supporting P3 access should conform to the MTS Access profile AMH23.

*Note: The above recommendation is to promote interoperability and support seamless operation. The above recommendation also implies conformance to the AMH12 MTS Access profile.*

**[AMHS-AMU-B09]** A UA should additionally implement the SEC Functional Group of the P3 Access profile AMH12/AMH14, for security class S0.

*Note 1: The above recommendation, if followed, enables authentication between ATS Message User Agent and ATS Message Server, and provides forward compatibility for secure messaging. ICAO Doc 9880 Part IIB states that SEC(S0) support is required for the Extended ATSMHS, but also implies that such support is conditional upon the ATSMHS SEC functional group. UA support of the SEC functional group for P3 is specified as optional for the EUR AMHS Profile in Appendix B Annex C and Annex G of ICAO EUR Doc 020 [8].*

*Note 2: Profiles AMH23/AMH25, which specify IPM requirements for P3 access, contain additional requirements for IPM Security, with additional security classes "SECn" (compared with "Sn" used in Common Messaging profiles). However, the Extended ATSMHS does not require IPM-specific Security functionality, only the Common Messaging SEC(S0) FG.*

*Note 3: Implementation of the SEC(S0) FG means that the UA supports and uses initiator-credentials and responder-credentials fields in the MTSBind operation for simple authentication (strong authentication may optionally be bilaterally agreed). It also means support (but not necessarily use) of the SubmissionControl element and the Message Token extension data type, including the signed-data element. Security related fields in submission and delivery envelopes are minimally supported, i.e. relayed transparently between MTA and UA.*

#### B.2.3.4 P7 Access

**[AMHS-AMU-B10]** A UA supporting P7 access shall conform to the profile in Appendix B Annex H, or Appendix B Annex I of ICAO EUR Doc 020 [8].

*Note: The referenced profile requires conformance to MHS Profile AMH13 or AMH15. It requires support of the optional DL functional group and the file transfer encoded information type. DL is only needed if dl-exempted-recipients is supported in the message submission envelope.*

**[AMHS-AMU-B11]** A UA supporting P7 access shall conform to the profile in Appendix B Annex D, or Appendix B Annex E of ICAO EUR Doc 020 [8], with the addition of support of the DIR Functional Group as specified in ICAO Doc 9880 Part IIB [5], section 3.1.4.3.1.

*Note: The referenced profile requires conformance to MHS Profile AMH24 or AMH26. It requires support of the DL functional group and the file transfer body part type.*

**[AMHS-AMU-B12]** It is recommended that a UA supporting P7 access should conform to the Enhanced MS Access profile AMH24.

*Note: The above recommendation is made to promote interoperability and support seamless operation. The above recommendation also implies conformance to the AMH13 MS Access profile.*

**[AMHS-AMU-B13]** A UA supporting P7 access should additionally implement the SEC Functional Group of the IPM P7 Access profile AMH24/AMH26, for security class S0 (only).

*Note 1: The above recommendation, if followed, enables authentication between ATS Message User Agent and ATS Message Server and provides forward compatibility for secure messaging. ICAO Doc 9880 Part IIB states that SEC(S0) support is required for the Extended ATSMHS, but also implies that such support is conditional upon the ATSMHS SEC functional group. UA support of the SEC functional group for P7 is specified as optional for the EUR AMHS Profile in Appendix B Annexes H, I, D and E of ICAO EUR Doc 020 [8].*

*Note 2: Implementation of the SEC Functional Group of profile AMH24/AMH26 also implies implementation of the SEC Functional Group of profile AMH13/AMH15.*

*Note 3: Basic conformance to AMH13 and/or AMH15 means that the UA supports and uses initiator-credentials and responder-credentials fields in the MSBind operation for simple authentication (strong authentication may optionally be bilaterally agreed). Conformance to the SEC Functional Group of profile AMH13/AMH15 requires support (but not necessarily use) of security fields in the message submission envelope, including the Message Token.*

**[AMHS-AMU-B14]** A UA supporting P7 access shall additionally implement the BC Functional Group of the IPM P7 Access profile AMH24/AMH26 as specified in ICAO Doc 9880 Part IIB [5], section 3.1.4.3.1, for the IPM heading fields indicated as “m” in Table B-1.

#### B.2.3.5 Directory Access

**[AMHS-AMU-B15]** An ATS Message User Agent implementing the DIR functional group shall include a DUA for access to the ATN Directory.

*Note 1: Annex C of this EUROCONTROL Specification specifies DUA requirements.*

*Note 2: As noted in ISO/IEC ISP 10611-1 [19], a directory may be used directly by MHS users to obtain information to assist in the submission of messages. However, such use is not necessarily MHS-specific and is therefore outside the scope of the ISP. For a UA, support of the DIR FG only requires the ability to submit a message with one or more OR-names specified using a directory name (DN). In addition, the UA is able to make use of a DN to identify itself. Whether or not the UA also has the capability to access a directory directly is outside the scope of the MHS standards.*

## B.2.4 Message Store Requirements

### B.2.4.1 General

*Note: The MS is an optional functional object in the AMHS logical architecture. For an MS in an ATS Message Server supporting the Extended ATSMHS, the access profiles are prescribed in ICAO Doc 9880 Part IIB [5].*

### B.2.4.2 MS Access to MTA

**[AMHS-MST-B01]** An MS which supports P3 access in an ATS Message Server supporting the Extended ATSMHS shall conform to the profile in Appendix B Annex G of ICAO EUR Doc 020 [8].

*Note: The referenced profile requires conformance to MHS Profile AMH12 and optionally also allows support of MHS Profile AMH14. It requires support of the DL functional group and the file transfer encoded information type.*

**[AMHS-MST-B02]** An MS which supports P3 access in an ATS Message Server supporting the Extended ATSMHS shall conform to the profile in Appendix B Annex C of ICAO EUR Doc 020 [8], with the addition of support of the DIR Functional Group as specified in ICAO Doc 9880 Part IIB [5], section 3.2.4.3.

*Note: The referenced profile requires conformance to MHS Profiles AMH23 and/or AMH25. It requires support of the DL functional group.*

**[AMHS-MST-B03]** It is recommended that an MS supporting P3 access should conform to the MTS Access profile AMH23.

*Note: The above recommendation is made to promote interoperability and support seamless operation. The above recommendation also implies conformance to the AMH12 MTS Access profile.*

**[AMHS-MST-B04]** An MS which supports P3 access should additionally implement the SEC Functional Group of the IPM P3 Access profile AMH23/AMH25, for security class S0.

*Note 1: MS support of the SEC functional group for P3 is specified as optional for the EUR AMHS Profile in Appendix B Annex C and Annex G of ICAO EUR Doc 020 [8].*

*Note 2: Implementation of the SEC Functional Group of profile AMH23/AMH25 also implies implementation of the SEC Functional Group of profile AMH12/AMH14, with the addition of support for certificates in the IPM message submission and delivery envelopes.*

*Note 3: The above recommendation means that the MS supports and uses initiator-credentials and responder-credentials fields in the MTSBind operation for simple authentication (strong authentication may optionally be bilaterally agreed). It also recommends support (but not necessarily use) of the SubmissionControl element and the Message Token extension data type, including the signed-data element. Security related fields in submission and delivery envelopes are minimally supported, i.e. relayed transparently between MTA and MTS-user.*

**[AMHS-MST-B05]** An MS which accesses the MTA by local means shall provide equivalent message submission and delivery functionality to that specified in the P3 access profile above.

*Note: Use of P3 is optional for an MS, and the MS-MTA interface would not normally be visible. However, the MS still needs to support the message submission and delivery information objects as used in the P3 abstract service.*

### B.2.4.3 P7 Access

**[AMHS-MST-B06]** An MS in an ATS Message Server supporting the Extended ATSMHS shall conform to the P7 access profile in Appendix B Annex H, or Appendix B Annex I of ICAO EUR Doc 020 [8] for message retrieval and indirect submission.

*Note: The referenced profile requires conformance to MHS Profile AMH13 or AMH15. It requires support of the optional DL functional group and the file transfer encoded information type. DL is only needed if dl-exempted-recipients is supported in the message submission envelope.*

**[AMHS-MST-B07]** An MS in an ATS Message Server supporting the Extended ATSMHS shall conform to the profile in Appendix B Annex D, or Appendix B Annex E of ICAO EUR Doc 020 [8], with the addition of support of the DIR Functional Group as specified in ICAO Doc 9880 Part IIB [5], section 3.1.4.3.1.

*Note: The referenced profile requires conformance to MHS Profile AMH24 or AMH26. It requires support of the DL functional group and the file transfer body part type. The choice between AMH24 and AMH26 depends on the functionality of the associated UA. Conformance to AMH24 implies conformance to AMH13. Conformance to AMH26 implies conformance to AMH15.*

**[AMHS-MST-B08]** An MS in an ATS Message Server supporting the Extended ATSMHS should additionally implement the SEC Functional Group of the IPM P7 Access profile AMH24/AMH26, for security class S0 (only).

*Note 1: MS support of the SEC functional group for P7 is specified as optional for the EUR AMHS Profile in Appendix B Annexes H, I, D and E of ICAO EUR Doc 020 [8].*

*Note 2: Implementation of the SEC Functional Group of profile AMH24/AMH26 also implies implementation of the SEC Functional Group of profile AMH13/AMH15.*

*Note 3: Basic conformance to AMH13 and/or AMH15 means that the MS supports and uses initiator-credentials and responder-credentials fields in the MSBind operation for simple authentication (strong authentication may optionally be bilaterally agreed). Conformance to the SEC Functional Group of profile AMH13/AMH15 requires support (but not necessarily use) of security fields in the message submission envelope, including the Message Token.*

**[AMHS-MST-B09]** An MS in an ATS Message Server supporting the Extended ATSMHS shall additionally implement the BC Functional Group of the IPM P7 Access profile AMH24/AMH26 as specified in ICAO Doc 9880 Part IIB [5], section 3.1.4.3.1 for the IPM heading fields indicated as “m” in Table B-1.

## B.2.5 AFTN/AMHS Gateway Requirements

### B.2.5.1 General

*Note: An AFTN/AMHS Gateway supporting the Extended ATSMHS includes an MTA, a DUA and an Access Unit (the Message Transfer and Control Unit – MTCU), as specified in ICAO Doc 9880 Part IIB [5] chapter 4.*

### B.2.5.2 Directory Access

**[AMHS-GWY-B01]** An AFTN/AMHS Gateway implementing the DIR functional group shall include a DUA for access to the ATN Directory.

*Note: Annex C of this EUROCONTROL Specification specifies DUA requirements.*

**[AMHS-GWY-B02]** It is recommended that the DUA in an AFTN/AMHS Gateway supporting the Extended ATSMHS should be used to retrieve information in support of address and content conversion.

*Note: The retrieval of directory information can be used by the MTCU to facilitate address conversion. The MTCU also requires further information on the level of service supported by the intended AMHS recipients.*

## B.3 CONFORMITY ASSESSMENT MATERIALS

This section includes the profile requirements list (PRL) for the communications services specified in Annex B.

### B.3.1 Compliance Statement

**[AMHS-CA-B01]** A claim of conformance for an implementation shall be supported by completion of the relevant Protocol Implementation Conformance Statement (PICS) pro forma.

**[AMHS-CA-B02]** Implementers claiming conformance to the specified services shall complete the PICS specified in Appendix B Annex Q of ICAO EUR Doc 020 [8], taking due account of the specific requirements for implementations of AMHS End Systems supporting the Extended ATSMHS specified in this Annex of the EUROCONTROL Specification.

*Note: For each AMHS system component the EUR AMHS profile specification in [8] contains a corresponding Implementation Conformance Statement (ICS) pro forma that is intended to document each implementation's conformance to the Base Standards, the referenced ISPs, the ICAO technical provisions and the corresponding EUR Profile Annexes.*

**[AMHS-CA-B03]** Implementers shall state whether all of the requirements and which of the optional elements of the AFTN/AMHS Gateway supporting the Extended ATSMHS as specified in ICAO Doc 9880 Part IIB [5] section 4 have been implemented, using the tables in this section or equivalent.

*Note: The following legend is used in Table B-2:*

M	=	Mandatory Support
C.a	=	At least one must be supported
O	=	Optional Support
I	=	Out of Scope
X	=	Excluded
-	=	Not applicable

**Table B-2: Profile requirements list for AFTN/AMHS Gateway supporting the Extended ATSMHS**

PRL Ref Extended	Question	Doc 9880 Part IIB Ref	Profile Req	Supplier Response	Notes
	<b>Subsetting Rules</b>	<b>3.4</b>			
1	<b>Classification of ATSMHS Functional Groups</b>	<b>Table 3-6</b>			
	Which of the following functional groups are supported?				
1.1	Basic ATS Message Handling Service		M		Basic
1.2	Use of File Transfer Body Parts for Binary data exchange		M		FTBP
1.3	Use of IPM Heading Extensions		M		IHE
1.4	AMHS Security		O		SEC
1.5	Use of Directory		M		DIR
	<b>Definition of ATSMHS subsets</b>	<b>Table 3-7</b>			
2	Which of the following subsets is supported?				

EUROCONTROL SPECIFICATION  
on the  
Air Traffic Services Message Handling System (AMHS)

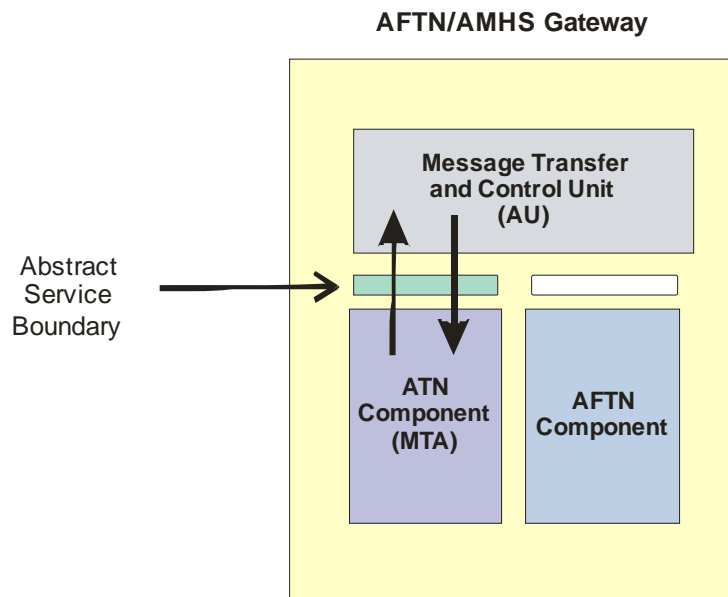
PRL Ref Extended	Question	Doc 9880 Part IIB Ref	Profile Req	Supplier Response	Notes
2.1	I. Basic ATS Message Handling Service (Basic)		M		
2.2	II. Basic + FTBP		-		
2.3	III. Basic + IHE		-		
2.4	IV. Basic + DIR		-		
2.5	V. Basic + DIR + FTBP		-		
2.6	VI. Basic + DIR + IHE		-		
2.7	VII. Basic + DIR + SEC		-		
2.8	VIII. Basic + IHE + DIR + SEC		-		
2.9	IX. Basic + IHE + DIR + FTBP		M		
2.10	X. Basic + IHE + DIR + FTBP + SEC		O		
<b>ATN Component</b>		<b>4.2.2</b>			
3	Which of the following Message Handling System optional functional groups are implemented?	4.2.2.4			
3.1	Conversion (CV)		O		
3.2	Distribution List (DL)		M		
3.3	Physical Delivery (PD)		O		
3.4	Redirection (RED)		O		
3.5	Latest Delivery (LD)		O		
3.6	Return of Contents (RoC)		O		
3.7	Security (SEC) Class:		O		
3.7.1	S0		M		
3.7.2	S1		X		
3.7.3	S2		X		
3.7.4	SnC		X		
3.8	Use of Directory (DIR)		M		
3.9	84 Interworking (84IW)		X		
3.10	If RED is implemented, does the ATN Component redirect messages and probes in the event that the MTCU is unable to accept them?	4.2.2.4.1	O		
3.11	If DL is implemented, does the ATN Component interface with the DUA component for DL-expansion?	4.2.2.8			
<b>Message Transfer and Control Unit</b>		<b>4.2.3</b>			
4	Does the MTCU interface with the gateway DUA component?	4.2.3.10	O		For the retrieval of address information for the purpose of address conversion

EUROCONTROL SPECIFICATION  
on the  
Air Traffic Services Message Handling System (AMHS)

PRL Ref Extended	Question	Doc 9880 Part IIB Ref	Profile Req	Supplier Response	Notes
	<b>Conversion of AFTN Acknowledgement Messages</b>	<b>4.4.3</b>			
5	Is the case of the user element of the IPM-identifier modified when constructing a RN?	4.4.3.3.3.1	O		
	<b>AMHS IPM Conversion</b>	<b>4.5.2</b>			
6	Is conversion from ISO 8859-1 to IA5IRV supported?	4.5.2.1.4 a) 4)	O		
7	Can the conversion be modified to support locally defined conversion rules?		O		
8	If recipient names cannot be translated into an AF-Address how many non-delivery reports are generated?	4.5.2.2.6.2.1			
8.1	One report for each failure		C.a		
8.2	A single report		C.a		
	<b>Generation of AMHS reports</b>	<b>4.5.6</b>			
9	Is a single non-delivery report generated on the rejection for multiple recipients?	4.5.6.1.2	O		
10	Is a single delivery report generated for multiple recipients?	4.5.6.1.4	O		
11	Is the case of the <i>global-domain-identifier</i> element of the <i>MTS-identifier</i> modified when constructing a report?	4.5.6.2.11.1	O		
12	Is the Return Of Content (RoC) Functional Group implemented in the MTCU?	4.5.6.2.16.1	O		
<b>AFTN/AMHS Gateway Control Position</b>		<b>4.2.6</b>			
13	Does the Control Position interface to the DUA component?	4.2.6.4	O		To allow the Control Position access to the ATN Directory
<b>DUA Component</b>		<b>4.2.7</b>			
14	Is the DUA Component used to retrieve information from the ATN Directory?	4.2.7.3	O		To support address conversion

*Note: ICAO Doc 9980 Part IIB expresses the functional requirements of the AFTN/AMHS Gateway component using tabular profile requirement lists which apply at the abstract service boundary between the ATN Component (MTA) and the MTCU of the AFTN/AMHS Gateway, as shown in Figure B-1.*





**Figure B-1: MTCU and ATN Component Abstract Service Boundary**

**[AMHS-CA-B04]** For AFTN/AMHS Gateway implementations, a PICS shall be provided stating the level of support, for each of the elements relevant to support of the Extended ATSMHS, listed in the profile requirements lists in section 4 of ICAO Doc 9880 Part IIB [5] and specified in Table B-3.

**Table B-3: MTCU Profile Requirements for the Extended ATSMHS**

Reference in ICAO Doc 9880 Part IIB	Description
Table 4-3	Specifies the required and optional elements for the generation of an IPM when converting a received AFTN message to AMHS. The column headed "ATS Mess. Service" in the referenced Table specifies the static capability requirements of an IPM AU supporting the ATSMHS. Elements marked with an asterisk (*) are applicable and elements marked as "C1" are mandatory for AFTN/AMHS Gateway implementations supporting the Extended ATSMHS level of service.
Table 4-4	Specifies the required and optional elements for the generation of a message transfer envelope when converting from AFTN to AMHS. The column headed "ATS Mess. Service" in the referenced Table specifies the static capability requirements of an IPM AU supporting the ATSMHS. Elements marked with an asterisk (*) are applicable for AFTN/AMHS Gateway implementations supporting the Extended ATSMHS level of service.
Table 4-6	Specifies the required and optional elements for the generation of an AMHS Receipt Notification resulting from the receipt of an AFTN acknowledgement message. The column headed "Basic ATS Mess. Service" in the referenced Table specifies the static capability requirements of an IPM AU.
Table 4-7	Specifies the required elements for the generation of a message transfer envelope for an AMHS Receipt Notification resulting from the receipt of an AFTN acknowledgement message. The column headed "Basic ATS Mess. Service" in the referenced Table specifies the static capability requirements of an IPM AU.

EUROCONTROL SPECIFICATION  
on the  
Air Traffic Services Message Handling System (AMHS)

---

Reference in ICAO Doc 9880 Part IIB	Description
Table 4-9	Specifies the required and optional elements for the generation of an AFTN message when converting from AMHS. The column headed "ATS Mess. Service" in the referenced Table specifies the static capability requirements of an IPM AU supporting the ATSMHS. Elements marked with an asterisk (*) are applicable for AFTN/AMHS Gateway implementations supporting the Extended ATSMHS level of service.
Table 4-10	Specifies the required support of elements in a received message transfer envelope when converting from AMHS to AFTN. The column headed "ATS Mess. Service" in the referenced Table specifies the static capability requirements of an AU in relation to the message transfer elements of service.
Table 4-12	Specifies the required support of elements in a received AMHS Receipt Notification when converting to an AFTN acknowledgement message. The column headed "Basic ATS Mess. Service" in the referenced Table specifies the static capability requirements of an IPM AU.
Table 4-13	Specifies the required support of elements in a message transfer envelope received with an AMHS Receipt Notification when converting to AFTN. The column headed "Basic ATS Mess. Service" in the referenced Table specifies the static capability requirements of an AU in relation to the message transfer elements of service.
Table 4-15	Specifies the required support of elements in a received AMHS Report when converting to an AFTN service message. The column headed "Basic ATS Mess. Service" in the referenced Table specifies the static capability requirements of an IPM AU.
Table 4-16	Specifies the required support of elements when generating an AMHS Report. The column headed "Basic ATS Mess. Service" in the referenced Table specifies the static capability requirements of an AU.

### B.3.2 Testing Requirements

**[AMHS-CA-B05]** AMHS End Systems supporting the Extended ATSMHS shall be tested according to suitable test cases and procedures ensuring adequate coverage of the IHE, FTBP and DIR functional groups.

**[AMHS-CA-B06]** Testing shall be conducted within a common framework consistent with the procedures in ICAO EUR Doc 020 [8] using appropriate test tools and procedures.

**EUROCONTROL SPECIFICATION**  
**on the**  
**Air Traffic Services Message**  
**Handling System (AMHS)**  
**ANNEX C - Directory**

**SPECIFICATION DOCUMENT IDENTIFIER: EUROCONTROL-SPEC-0136**

<b>Edition Number</b>	<b>:</b>	<b>2.0</b>
<b>Edition Date</b>	<b>:</b>	<b>18/09/2009</b>
<b>Status</b>	<b>:</b>	<b>Released</b>
<b>Intended for</b>	<b>:</b>	<b>General Public</b>
<b>Category</b>	<b>:</b>	<b>EUROCONTROL Specification</b>

## DOCUMENT CHANGE RECORD

The following table records the complete history of the successive editions of the present document.

EDITION NUMBER	EDITION DATE	INFOCENTRE REFERENCE	REASON FOR CHANGE	PAGES AFFECTED
0.1	16/01/08		Initial outline	All
0.2	25/01/08		Detail added	All
0.3	26/02/08		Further evolution. Input to Drafting Group	All
0.4	01/04/08		Further evolution. Comments from drafting group 29/02/08.	All
0.5	13/06/08		Draft for Review Group	All
0.6	24/10/08		Updated after informal stakeholder review. Was previously Annex B.	All
1.0	08/12/08		Updated after informal stakeholder review. Input to formal consultation.	All
1.1	27/07/09		Updated after ENPRM-09/001 formal consultation.	All
2.0	18/09/09		Released Issue	Footers

## CONTENTS

<b>ANNEX C - DIRECTORY REQUIREMENTS .....</b>	<b>1</b>
<b>C.1. CONFIGURATION CONTROL .....</b>	<b>1</b>
C.1.1 MOC Element Identification .....	1
C.1.2 MOC Element Change Record .....	1
C.1.3 MOC Element Traceability Towards Regulatory Provisions .....	1
C.1.4 MOC Element Traceability towards International Standards .....	1
<b>C.2. REQUIREMENTS AND EXPLANATORY MATERIALS .....</b>	<b>2</b>
C.2.1 General Directory Requirements .....	2
C.2.1.1 Architecture .....	2
C.2.1.2 Directory User Agent access .....	3
C.2.1.3 Directory Contents Access Policy .....	4
C.2.2 AMHS-Specific Directory Requirements .....	4
C.2.2.1 Directory Functions in support of AMHS .....	4
C.2.2.2 Directory Information in support of AMHS .....	6
C.2.2.3 Simple AMHS Address Conversion Directory Algorithm .....	7
C.2.3 Directory support of PKI .....	10
C.2.4 System capacity and performance .....	10
<b>C.3. CONFORMITY ASSESSMENT MATERIALS .....</b>	<b>11</b>
C.3.1 Object Class Requirements .....	11
C.3.2 Attribute Requirements .....	12
C.3.3 List of X.500 Global Statement and Protocol Operations Supported by the Directory Service .....	14
C.3.4 Requirements Statement for DUAs .....	15
C.3.5 Requirements Statement for DSAs .....	17
C.3.6 Requirements Statement for Conformance by a Shadow Supplier .....	20
C.3.7 Requirements Statement for Conformance by a Shadow Consumer .....	21



## ANNEX C – DIRECTORY REQUIREMENTS

### C.1. CONFIGURATION CONTROL

#### C.1.1 MOC Element Identification

MOC_Name	MOC_Version	MOC_Edition
AMHS_DIR	1	1

#### C.1.2 MOC Element Change Record

The following table records the complete history of the successive editions of MOC specifications.

Version Number	Edition Number	Edition Date	Reason for Change	Sections Affected
1	1	18/09/09	Initial specification	All

#### C.1.3 MOC Element Traceability Towards Regulatory Provisions

The following table records the traceability history of regulatory provisions associated with this MOC element.

Version Number	Edition Number	Implementing rule references	References of regulatory provisions	Validation date
1	1	N/A	Regulation (EC) No 552/2004 [1] Annex II Part A and Part B (4) - Essential requirements applicable to communications systems and procedures for ground-to-ground communications	22/10/08

#### C.1.4 MOC Element Traceability towards International Standards

The following table records the traceability of international standards associated with this MOC element.

International standards identification	References of text parts used to draft MOC specifications	References of text parts imported into the MOC
ICAO Doc 9880 Part IIB [5]		Functional group DIR
ICAO Doc 9880 Part IVA [7]		Whole document

## C.2. REQUIREMENTS AND EXPLANATORY MATERIALS

*Note 1: This normative Annex is an integral part of this EUROCONTROL Specification. It specifies requirements for the use of Directory service by AMHS. The scope of this Annex is:*

- a) to define the basis of a general directory service that could be used to share information generally in the EATMN (section C.2.1);*
- b) to define specific requirements for the use of the directory service to support AMHS (section C.2.2);*
- c) to define specific requirements for the use of the directory service to support the public key infrastructure (PKI) to support AMHS security service (section C.2.3), if required.*

*Note 2: This Annex must be read in conjunction with the Main Body of this EUROCONTROL Specification, which provides definitions, document references and contextual information. References given in square brackets are defined in section 10 of the Main Body.*

### C.2.1 General Directory Requirements

*Note 1: This section describes the generic/common part of the directory service to be used in support of the Extended ATSMHS, but that may also be used by other ATM services outside of the scope of this EUROCONTROL Specification.*

*Note 2: The Directory system consists of one or more Directory System Agents (DSAs), accessed from Directory User Agents (DUAs) via an access protocol. The Directory Access Protocol (DAP) is currently the only access protocol specified by ICAO. Where multiple DSAs cooperate to provide a distributed directory service, the Directory System Protocol (DSP) can be used to support chaining (passing a query to another DSA when it cannot be resolved locally) and referrals (returning a reference to another DSA when a query cannot be resolved locally). The Directory Information Shadowing Protocol (DISP) may be used to replicate shared parts of the Directory Information Tree (DIT) between DSAs.*

*Note 3: Due to operational requirements which have yet to be resolved, the Directory structure in Europe may include additional elements beyond those specified in current ICAO documentation. This would include, for example, additional attributes for version control.*

**[AMHS-DIR-C01]** AMHS End Systems supporting the DIR functional group shall include access to directory information as specified in the schema defined in ICAO Doc 9880 Part IVA [7].

**[AMHS-DIR-C02]** The directory functionality shall comply with the standards and ISPs referenced from ICAO Doc 9880 Part IVA [7].

*Note: These ICAO provisions are in turn based on ISO/IEC 9594 [34] standards, which are technically aligned with ITU-T X.500 Recommendations.*

**[AMHS-DIR-C03]** Directory protocols shall operate over the TCP transport service as specified in ICAO Doc 9880 Part IVA [7], section 5.7.6.3.

#### C.2.1.1 Architecture

*Note: This section describes a directory architecture for the EATMN and details requirements met by the directory systems in order to guarantee interoperability and data sharing.*

**[AMHS-DIR-C04]** In order to guarantee the consistency of the shared part(s) of the DIT, it shall be ensured that each DSA:



- a) has a common view of the schema for the shared data,
- b) supports a common means of directory replication and/or chaining / referral of queries,
- c) does not require any modification of the data replicated from other DSAs.

**[AMHS-DIR-C05]** The DSA shall implement DSP to support the exchange of data with other DSAs.

**[AMHS-DIR-C06]** The DSA should implement DISP including support for incremental and full shadow updates, supplier and consumer initiated, scheduled and on-change updates, attribute filtering and chop shadowing.

**[AMHS-DIR-C07]** The DSA shall support the bind operation using as a minimum simple authentication for DAP, DSP and DISP as defined in the base standards.

**[AMHS-DIR-C08]** The DSA should additionally support the bind operation using strong authentication for DAP, DSP and DISP as defined in the base standards.

**[AMHS-DIR-C09]** The Directory service implementation shall allow additional directory object classes and attributes to be included in order to allow the use of this service by other applications within the scope of other private or EATMN directory service deployment.

**[AMHS-DIR-C10]** The DSA shall have the ability to export and import directory information in Lightweight Directory Access Protocol Interchange Format (LDIF) format, where applicable.

*Note: This is required to enable implementation of the initial directory architecture. LDIF is a standard plain text data interchange format for representing LDAP (Lightweight Directory Access Protocol) directory content and update requests. It is specified in RFC 2849 [42].*

### **C.2.1.2 Directory User Agent access**

*Note: This section describes characteristics of the directory to support DUAs.*

**[AMHS-DIR-C11]** The DSA shall implement DAP to support user access to the directory information.

*Note: The above is the minimum requirement for standardised access to the ATN Directory. It does not preclude the implementation of additional access mechanisms in individual cases.*

**[AMHS-DIR-C12]** The DSA may also implement other access protocols based on LDAP [39] or a proprietary protocol to support user access to the directory information.

**[AMHS-DIR-C13]** If DAP or LDAP is implemented by the DUA, the use of “referral” identifying a DSA external to the EATMN should be strictly controlled.

*Note: It may be required to prevent a DUA from one country requiring direct access to a DSA in a foreign country.*

### C.2.1.3 Directory Contents Access Policy

*Note: This section describes the need for defining different directory content access policies, e.g. public information (shared with other States/Organisations), and different privacy groups of users for internal directory data.*

**[AMHS-DIR-C14]** It shall be possible to define access control policy in order to regulate what type of operation can be performed on a directory entry, attributes or values.

**[AMHS-DIR-C15]** The basic operations listed in Table C-1 shall be supported by DUAs and DSAs.

**Table C-1: Directory Access Operations**

<b>Operation</b>	<b>Description</b>
Read	Retrieve the information contained in an entry, as specified by its Distinguished Name;
Compare	Compare a user-supplied attribute value against one held in an entry, as specified by its Distinguished Name;
List	List the subordinate entries of an entry, as specified by its Distinguished Name;
Search	Search through all the subordinate entries of an entry, as specified by its Distinguished Name, returning those entries which match specified criteria;
Add Entry	Add a new entry to the Directory Information Base, specifying the new entry's name and contents;
Remove Entry	Delete an entry from the Directory Information Base, as specified by its Distinguished Name;
Modify Entry	Modify the contents of a Directory entry, as specified by its Distinguished Name, specifying the desired modifications;
Modify DN	Change the Relative Distinguished Name (RDN) of an entry, as specified by its Distinguished name, or move it to a new superior in the DIT, or both.

### C.2.2 AMHS-Specific Directory Requirements

*Note: This section describes directory service requirements linked to AMHS.*

#### C.2.2.1 Directory Functions in support of AMHS

**[AMHS-DIR-C16]** The Directory implementation shall support the following functions:

- a) **Name resolution:** This function consists of converting the O/R-name of an AMHS user that takes the form of a Directory-name into the O/R-address of this AMHS user. This function is used to perform message-submission and probe-submission procedures when the O/R-Name of the message or the recipient-Name of the probe only contains the directory name. This will ultimately include support of name resolution for addresses from other domains;
- b) **Distribution list (DL) expansion and management:** An MTA can manage the distribution lists it hosts by means of directory information. The members and characteristics of the DL stored in the directory are used at the moment of DL-expansion;
- c) **Determination of recipient (direct/indirect DUA or DL) capabilities:** this function consists of retrieving information about an intended recipient, identified by a directory name, prior to message submission/transfer. Such information could include, for

example, maximum deliverable message length, support for Extended ATSMHS, etc. This information can be used to determine if delivery of a message to the intended recipients is possible or not.

- d) AFTN/AMHS address conversion and publication:** This function provides information in support of conversion of an AFTN address into an O/R-address and vice-versa, as required by an AFTN/AMHS gateway. The same information is also useful for message generation;

**[AMHS-DIR-C17]** The Directory implementation should additionally support the following function, if required:

- e) Retrieval of security certificates and CRLs;** This function is used by ATS Message User Agents and AFTN/AMHS Gateways implementing AMHS Security at the moment of verification of the ATN signature. This function consists of storing public key information of AMHS users in the form of user certificate and certificate revocation list (CRL).

**[AMHS-DIR-C18]** The Directory implementation may additionally support one or more of the following functions:

- f) Support for system configuration:** this function consists of storing the configuration of AMHS components (MTA, MTCU, UA) in order to allow maintenance via the directory. This function is not specified in ICAO Doc 9880 Part IVA, but is sometimes implemented in directory systems associated with message handling.
- g) AMHS systems management information:** ICAO Doc 9880 Part IVA [7] includes a number of object classes and attribute types that provide systems management information. This function is specified in ICAO technical provisions, but rarely implemented by X.500 product providers.
- h) Address book:** this function allows definition of a set of “regular recipients” that can be used by multiple users at a single location. This function is not specified in ICAO Doc 9880 Part IVA, but is commonly implemented in directory systems.

*Note 1: Some of the above functions do not need to use data imported from other Directory Management Domains (DMDs): “Address book” and “Support for system configuration”. These functions do not require common structure definitions shared between directories, and their implementation can be a local matter. While not concerned with technical interoperability between systems, a common set of functions will aid interoperability in the wider, procedural sense.*

*Note 2: The “AMHS systems management information” function uses data imported from other DMDs, but this function is not mandatory for the correct functioning of AMHS communications.*

**[AMHS-DIR-C19]** AMHS End System support of the directory functions shall be as indicated in Table C-2.

**Table C-2: Directory functions per AMHS End System type**

Directory functions	ATS Message User Agent	AFTN/AMHS Gateway	ATS Message Server
Name resolution	yes	yes	yes
Distribution list (DL) expansion and management		yes	yes
Determination of recipient capabilities	yes	yes	yes

Directory functions	ATS Message User Agent	AFTN/AMHS Gateway	ATS Message Server
AFTN/AMHS address conversion and publication	optionally	yes	
Retrieval of security certificates and CRLs	optionally	optionally	
AMHS systems management information (*)			
Address book	optionally		
Support for system configuration (MTA, Gateway)	optionally	optionally	optionally

(\*) The AMHS systems management information function should only be used by AMHS operators for “monitor” operations.

### C.2.2.2 Directory Information in support of AMHS

*Note: This section defines the data sub tree exported/imported by participating DMDs in order to support the directory functions useful for AMHS: Name resolution, DL expansion and management, Determination of recipient capabilities, AFTN/AMHS address conversion and publication, Retrieval of security certificates and CRLs.*

**[AMHS-DIR-C20]** The Directory information tree exported by Border DSAs shall conform to the DIT structure defined in ICAO Doc 9880 Part IVA [7], unless otherwise stated in this section.

*Note: The object classes defined in ICAO Doc 9880 Part IVA [7] are used to support several air-ground and ground-ground ATN applications. For AMHS support, the directory does not need to implement all of the information objects defined in the ICAO specification. The minimum required subset of these objects and attributes is specified in sections C.3.1 and C.3.2 below.*

**[AMHS-DIR-C22]** It is recommended that the DSA should export only *atn-amhs-user* and *atn-amhs-distribution-list* object-classes for users which have the capability to send/receive AMHS messages to/from other ATSMHS users.

**[AMHS-DIR-C23]** It is recommended that the exported / imported sub-trees should be attached to the country root DIT.

**[AMHS-DIR-C24]** The DSA shall use this DIT structure to support the name resolution function, using *Country*, *Organization*, *atn-organization* and *atn-amhs-user* object-classes.

**[AMHS-DIR-C25]** The DSA shall use this DIT structure to support the DL expansion and management function, with MTAs accessing members of the *atn-amhs-distribution-list* object-class.

**[AMHS-DIR-C26]** The DSA shall use this DIT structure to support the AFTN/AMHS address conversion function performed by the AFTN/AMHS Gateway based on the “Simple AMHS address conversion directory algorithm” described below, using object classes *Country*, *Organization*, *atn-organization*, *atn-amhs-user*, *atn-amhs-distribution-list* and *atn-amhsMD*.

**[AMHS-DIR-C27]** The attribute *description* of the object classes *Country* and *Organization* used as the root of the exported sub-tree shall be used as follows to store the current version of this sub-tree:

Format of the *description* attribute: "<version number> - <description of the object>".

**[AMHS-DIR-C28]** The country or the organization shall maintain the version of its exported sub-tree.

*Note: The "Common Off-line function" or the "Europe DSA" will be responsible to maintain the version of the sub-tree starting with the organization "O=ICAO-MD-Registry".*

### C.2.2.3 Simple AMHS Address Conversion Directory Algorithm

*Note: Based on the DIT structure outlined in section 4 of the Main Body the following algorithm is applicable for the AFTN/AMHS address conversion function:*

**[AMHS-DIR-C29]** Each DSA shall include:

- a) the subtree for its own ANSP containing local AMHS user information relative to AFTN/AMHS address translation,
- b) the MD-registry sub tree starting with a member of the *organization* object-class named O=ICAO-MD-Registry and containing *atn-amhsMD* objects (ideally replicated from a master DSA managed by ICAO),
- c) a replicated sub tree or a reference to the other ANSP exported DIT.

**[AMHS-DIR-C30]** The Directory information shall support address conversion between AMHS and AFTN address types.

*Note: For performance reasons, it is assumed that MTCU implementations will maintain a local address conversion storage capability. This may be populated by caching addresses obtained via the DUA, by replication of DIT subtrees, or by other means.*

**[AMHS-DIR-C31]** An O/R Address (MF-Address) included in an AMHS message shall be processed for translation into the AFTN address in one of four mutually exclusive manners, depending on the MF-Address format, after preliminary conversion of all address attribute values to upper case characters:

- a) Look up the MF-Address in the local address storage maintained in the MTCU. If an exact match is found, then extract the corresponding AF-Address, if present. In case information for a given user cannot be found, then an on-line query can be activated to retrieve information from the distributed ATN directory.
- b) if a) cannot be achieved, and the MF-Address to be converted is a CAAS-compliant address including a syntactically valid AF-Address as a *common-name* value, then:
  - 1) Extract the AF-Address found as the *common-name* value, and
  - 2) Perform a consistency check by re-converting this AF-Address as specified in **[AMHS-DIR-C32]** and comparing this with the MF-Address being converted. In case of discrepancy, log the error and report to a control position; or
- c) if a) cannot be achieved, and the MF-Address to be converted is an XF-Address including an *organizational-unit-names* value which is a syntactically valid AF-Address, then:
  - 1) Extract the AF-Address found as *organizational-unit-names* value, and
  - 2) Perform a consistency check by re-converting this AF-Address as specified in **[AMHS-DIR-C32]** and comparing this with the

MF-Address being converted. In case of discrepancy, log the error and report to a control position; or

- d) if none of the conditions in a), b) and c) can be met, notify the failure to translate the MF-Address.

[AMHS-DIR-C32]  
be supported:

For AFTN to AMHS address conversion, the following algorithm shall

- a) Look up the AF-Address in the local address storage maintained in the MTCU. If an exact match is found, then extract the corresponding MF-Address. In case information for a given user cannot be found, then an on-line query can be activated to retrieve information from the distributed ATN directory; or

- b) if a) cannot be achieved, translation from the AF-Address as follows:

- 1) Determine the country-name, administration-domain-name and private-domain-name address attributes belonging to the single AMHS MD, if any, among the entries of the ICAO-MD-Registry tree, where the *atn-icao-designator* attribute matches exactly the following character substrings of the AF-Address. If several matches are found then select on the basis of a decreasing order of precedence from i) to iv):

- i. characters 1 to 7,
- ii. characters 1, 2, 5, 6 and 7,
- iii. characters 1, 2, 3 and 4,
- iv. characters 1 and 2; and

- 2) determine the other O/R address attributes according to one of the following methods, depending on the addressing scheme declared by the AMHS MD determined as in item 1) above, and found in the MTCU's local address storage (attribute *atn-amhsMD-addressing-scheme* of the *atn-amhsMD* directory object):

- i. if the AMHS MD has selected the CAAS:
  - a) Use the *country* sub-tree identified during step 1) (using the *atn-amhsMD-naming-context* attribute), search this *country* sub-tree for the *atn-organization* object whose *Organization-Name* attribute value matches the Location Indicator of the AF-Address. Allocate the *atn-facility-name* of this object to the *organization-name* of the computed MF-Address,
  - b) Allocate the value of the Location Indicator from the AF-Address to the *organizational-unit-names* field of the computed MF-Address,
  - c) Allocate the AF-Address to the *common-name* field of the computed MF-Address.
- ii. if the AMHS MD has selected the XF addressing scheme, allocate the AF-Address to the *organizational-unit-names* field and allocate the string "AFTN" to the *organization-name* field.

- c) if none of the conditions in a) and b) can be met, notify the failure to translate the AF-Address.

*Note 1: The following examples illustrate address conversion using the above algorithm for an assumed AMHS MD sub-tree with the following contents:*

<b>atn-amhsMD attribute types and values</b>					
<b>Id</b>	<b>common-name</b>	<b>atn-global-domain-identifier</b>	<b>atn-icao-designator</b>	<b>atn-amhsMD-naming-context</b>	<b>atn-amhsMD-addressing-scheme</b>
1	CFMU_EUCH	/C=XX/A=ICAO/ P=EUROCONTROL-CFMU	EUCH	O=CFMUH	caas
2	BELGIUM	/C=XX/A=ICAO/P=BELGIUM	EB	C=BE	caas
3	FRANCE	/C=XX/A=ICAO/P=FRANCE	LF	C=FR	caas
4	WM	/C=XX/A=ICAO/P=WM	WM	C=WM	xf
5	CFMU_EUCBZM FP	/C=XX/A=ICAO/ P=EUROCONTROL-CFMU	EUCBZMF P	O=CFMUB	caas
...	CFMU_EUCBZK.. .	/C=XX/A=ICAO/ P=EUROCONTROL-CFMU	EUCBZK...	O=CFMUB	caas
31	CFMU_EUCBZKT	/C=XX/A=ICAO/ P=EUROCONTROL-CFMU	EUCBZKT	O=CFMUB	caas

*Note 2: Example AFTN address to AMHS address conversion:*

To convert AFTN address EUCHZMFP to AMHS, the address conversion function performs the following actions:

1. search in the O=ICAO-MD-Registry sub-tree for an atn-amhsMD object with an atn-icao-designator attribute value providing the best match with the AFTN address for the specified substrings: the first entry from the table above is selected.
2. extract supported addressing scheme from the atn-amhsMD object found: caas
3. search into the AMHS directory tree pointed by the atn-amhsMD-naming-context attribute for an atn-organization object with CN=EUCH (Location Indicator from the AFTN address).
4. Construct the AMHS address with the value of the atn-global-domain-identifier attribute of the atn-amhsMD object (C, A, P), the atn-facility-name of the atn-organization object (O), the Location Indicator extracted from the AFTN address (OU) and the AFTN address (CN):

/C=XX/A=ICAO/P= EUROCONTROL-CFMU/O=CFMUH/OU1=EUCH/CN=EUCHZMFP

*Note 3: Example AMHS address to AFTN address conversion:*

To convert AMHS address /C=XX/A=ICAO/P=WM/O=AFTN/OU1=WMKKZTZX to an AF-Address, the address conversion function performs the following actions:

1. Recognise that the O/R address is not in CAAS address format, but is in XF address format.
2. Extract the AFTN address from the OU1 field of the AMHS address: WMKKZTZX
3. Perform a consistency check by re-converting this AF-Address to an MF-Address as in Note 2 above and comparing this with the MF-Address being converted.

**[AMHS-DIR-C33]** States supporting the CAAS scheme within the EATMN should register values of the "Organization Name" field with length not exceeding 8 characters.

*Note: The above requirement is good practice to accommodate an initial limitation of the defined ATN Directory schema, whereby the atn-FacilityName attribute (of the atn-organization object) is limited to 8 characters while the "Organization Name" field permits up to 64 characters. atn-FacilityName is used by the AFTN/AMHS address translation algorithm to construct the field "Organization Name" of an AMHS O/R-address for CAAS countries.*

### **C.2.3 Directory support of PKI**

*Note: This section describes directory service requirements linked to PKI.*

**[AMHS-DIR-C34]** When being used to provide Directory support for PKI, the DSA shall use the specified DIT structure to provide support for retrieval of security certificates and CRLs, using *atn-amhs-user* (attribute *atn-der-certificate*) and *atn-certification-authority* object-classes.

### **C.2.4 System capacity and performance**

**[AMHS-DIR-C35]** The DSA design should be scalable in a cost effective manner in order to be able to store more AMHS information and support additional DUA directory operations.

*Note: The ATN directory needed to support the Extended ATSMHS will eventually need to hold an entry for every AMHS user in the world. This has been estimated to be around 80,000 users.*



### C.3. CONFORMITY ASSESSMENT MATERIALS

*Note: This section specifies the Profile Requirements List (PRL) for the services specified in this Annex.*

#### C.3.1 Object Class Requirements

**[AMHS-CA-C01]** DSAs shall implement as a minimum the object classes specified in Table C-3 to Table C-6, in order to guarantee correct understanding of the data shared between DMDs.

**Table C-3: DSA Supported ISO/IEC 9594-7:1995 Object Classes as Specified in ISO/IEC ISP 15126-1 [16]**

Ref. No	Object Class	ATN DSA	Support required	Comments
1	top	m	m	
2	alias	m	m	
3	country	m	m	
4	locality	m	o	
5	organization	m	m	
6	organizationUnit	m	o	
7	person	m	o	
8	organizationalPerson	m	o	
9	organizationalRole	m	o	
10	groupOfNames	o	o	
11	groupofuniqueNames	o	o	
12	residentialPerson	o	o	
13	applicationProcess	m	o	
14	applicationEntity	m	o	
15	dSa	m	o	
16	device	m	o	
17	strongAuthenticationUser	m	o	
18	certificationAuthority	m	m	

**Table C-4: DSA supported Object Classes Defined in ISO/IEC ISP 15126-1 [16]**

Ref. No	Object Class	ATN DSA	Support required	Comments
1	ispApplicationEntity	o	o	

**Table C-5: DSA Object Classes Defined for Message Handling System (MHS) in ISO/IEC ISP 11189 (FDI2) [17]**

Ref. No	Object Class	ATN DSA	Support required	Comments
1	mhs-distributionList	m	m	
2	mhs-message-store	m	o	
3	mhs-message-transfer-agent	m	o	
4	mhs-user	m	m	
5	mhs-user-agent	m	o	

**Table C-6: DSA Object Classes Defined in ATN Directory [7]**

Ref. No	Object Class	ATN DSA	Support required	Comments
1	atn-amhs-user	m	m	
2	atn-organizational-unit	m	o	
3	atn-organizational-person	m	o	
4	atn-organizational-role	m	o	
5	atn-application-entity	m	o	
6	atn-certification-authority	m	m	
7	atn-amhs-distribution-list	m	m	
8	atn-amhs-user-agent	m	o	
9	atn-amhs-gateway	m	o	
10	atn-aircraft	m	o	
11	atn-facility	m	o	
12	atn-amhsMD	m	m	
13	atn-idrp-router	m	o	
14	atn-dSA	m	o	
15	atn-organization	m	m	

### C.3.2 Attribute Requirements

**[AMHS-CA-C02]** Table C-7 specifies the attributes that shall be used in support of the ATS Message Handling Service for each required object class.

*Note: The way that successive versions of attribute values can be managed is out of the scope of the Directory standards. Versioning of the directory data will be handled by local means.*

**Table C-7: Supported Attributes**

Object class	attribute	Support required	Comments
alias			
	aliasEntityName	Y	
country			
	countryName	Y	
	description	Y	
	searchGuide	O	
atn-amhs-user (sub-class of top, derived from mhs-user in ISO/IEC 10021-2)			
	mhs-maximum-content-length	Y	
	mhs-deliverable-content-types	Y	
	mhs-acceptable-eits	Y	
	mhs-exclusively-acceptable-eits	Y	
	mhs-message-store-dn	O	Support of MS is optional
	mhs-or-addresses	Y	
	mhsPreferredDeliveryMethods	Y	
	atn-per-certificate	N	
	atn-der-certificate	Y	
	atn-ipm-heading-extensions	Y	
	atn-amhs-direct-access	Y	
	atn-AF-address	Y	

EUROCONTROL SPECIFICATION  
on the  
Air Traffic Services Message Handling System (AMHS)

atn-certification-authority (sub class of certificationAuthority, which is defined in X.521)		
authorityRevocationList	Y	
cACertificate	Y	
certificateRevocationList	Y	
crossCertificatePair	Y	
atn-per-certificate	N	
atn-der-certificate	Y	

atn-amhs-distribution-list (sub class of mhs-distributionList, defined in ISO/IEC 10021-2)		
commonName	Y	
description	Y	
mhs-deliverable-content-types	Y	
mhs-acceptable-eits	Y	
mhs-exclusively-acceptable-eits	Y	
mhs-unacceptable-eits	O	
mhs-dl-submit-permissions	Y	
mhs-or-addresses	Y	
mhs-PreferredDeliveryMethods	Y	
organizationName	Y	
organizationalUnitName	N	
owner	Y	
seeAlso	O	
mhs-maximum-content-length	Y	
mhs-dl-policy	O	
mhs-dl-subscription-service	O	
mhs-dl-archive-service	O	
mhs-dl-related-lists	O	
mhs-dl-members	Y	
atn-ipm-heading-extensions	Y	
atn-PerCertificate	N	
atn-DerCertificate	N	

atn-amhsMD		
common-name	Y	
atn-global-domain-identifier	Y	
atn-icao-designator	Y	
atn-amhsMD-addressing-scheme	Y	
atn-amhsMD-naming-context	O/Y	Y if atn-amhsMD-addressing-scheme is CAAS

atn-organization (sub class of organization, which is defined in X.521)		
organizationName	Y	
organizationalAttributeSet	O	
atn-facility-name	Y	
atn-per-certificate	N	
atn-der-certificate	N	

### C.3.3 List of X.500 Global Statement and Protocol Operations Supported by the Directory Service

[AMHS-CA-C03] Table C-8 specifies the overall conformance and protocol operations that shall be used in support of the ATS Message Handling Service for each mandatory object class.

*Note: The DUA categories Administrative DUA, Operational Personnel DUA and Autonomous Operational DUA are defined in ICAO Doc 9880 Part IVA, section 1.3.12. The DUA component of the ATS Message Server, ATS Message User Agent and AFTN/AMHS Gateway belongs to the latter category. The other categories are necessary for directory administration.*

**Table C-8: X.500 Global Statement and Protocol Operations Supported by the Directory Service**

Operations	Ref	DSA	Autonomous Operational DUA	Operational Personnel DUA	Administrative DUA
<b>global conformance statement</b>					
Support of Basic Access control	X.501	m	-	-	-
Support of "simple" authentication procedure	X.509	m	o	o	o
Support of "strong" authentication procedure	X.509	o	o	o	o
<b>DISP Operations</b>					
DSA Shadow Bind	X.525	o	-	-	-
DSA Shadow UnBind	X.525	o	-	-	-
Coordinate Shadow Update	X.525	o	-	-	-
Request Shadow update	X.525	o	-	-	-
Update Shadow	X.525	o	-	-	-
<b>DSP Operations</b>					
Directory bind	X.511- X.518	m	-	-	-
Directory unbind	X.511- X.518	m	-	-	-
Chained Read	X.511- X.518	m	-	-	-
Chained Compare	X.511- X.518	m	-	-	-
Chained Abandon	X.511- X.518	m	-	-	-
Chained List	X.511- X.518	m	-	-	-
Chained Search	X.511- X.518	m	-	-	-
Chained Add Entry	X.511- X.518	o	-	-	-
Chained Remove Entry	X.511- X.518	o	-	-	-
Chained Modify Entry	X.511- X.518	o	-	-	-
Chained Modify DN	X.511- X.518	o	-	-	-
<b>DAP Operations</b>					
Directory bind	X.511	m	m	m	m
Directory unbind	X.511	m	m	m	m
Read	X.511	m	m	m	m

EUROCONTROL SPECIFICATION  
on the  
Air Traffic Services Message Handling System (AMHS)

Operations	Ref	DSA	Autonomous Operational DUA	Operational Personnel DUA	Administrative DUA
Compare	X.511	m	m	m	m
Abandon	X.511	m	m	m	m
List	X.511	m	m	m	m
Search	X.511	m	m	m	m
Add Entry	X.511	m	-	-	m
Remove Entry	X.511	m	-	-	m
Modify Entry	X.511	m	-	-	m
Modify DN	X.511	m	-	-	m

### C.3.4 Requirements Statement for DUAs

**[AMHS-CA-C04]** Implementers shall state whether all of the requirements and which of the optional elements of the DUA supporting the Extended ATSMHS, as specified in ICAO Doc 9880 Part IVA [7] section 5.2.1, have been implemented, using the table in this section or equivalent.

*Note: The following table is derived from the X.500 conformance specifications taken from section 13.1.1 of ISO/IEC 9594-5 | ITU-T Rec. X.519 (2005) [34].*

**Table C-9: Directory User Agent Requirements**

X.500 Conformance Statement Requirements	Profile	Notes
a) the operations of the <b>directoryAccessAC</b> application-context that the DUA is capable of invoking for which conformance is claimed	<b>See DAP Operations in Table C-8</b>	
b) the bind security level(s) for which conformance is claimed none simple, without password simple, with password simple, with protected-password strong Can the DUA generate signed arguments or validate signed results?	<b>m</b> – simple, with password  <b>o</b> - others	

EUROCONTROL SPECIFICATION  
on the  
Air Traffic Services Message Handling System (AMHS)

X.500 Conformance Statement Requirements	Profile	Notes
<p>c) the extensions listed Table 1 of ITU-T Rec. X.511   ISO/IEC 9594-3, that the DUA is capable of initiating for which conformance is claimed;</p> <p>subentries copyShallDo attribute size limit extraAttributes modifyRightsRequest pagedResultsRequest matchedValuesOnly extendedFilter targetSystem useAliasOnUpdate newSuperior manageDSAIT useContexts partialNameResolution overspecFilter selectionOnModify Security parameters - Response Security parameters - Operation code Security parameters - Attribute certification path Security parameters - Error Protection SPKM Credentials Bind token - Response Bind token - Bind Int. Alg, Bind Int Key, Conf Alg and Conf Key Info Bind token - DIRQOP Service administration entryCount hierarchySelection relaxation familyGrouping familyReturn dnAttributes</p>	<p>O - all</p>	
<p>d) Is conformance claimed to Rule-based Access Control? (capability of supporting security labels as identified in 19.4 of ITU-T Rec. X.501   ISO/IEC 9594-2)</p>	<p>o</p>	
<p>e) Identification of the Certificate and CRL extensions for which conformance is claimed. (Conformity to clauses 8 and 15 of ITU-T Rec. X.509   ISO/IEC 9594-8)</p>	<p><b>c –</b> <u>Supported certificate extensions:</u> keyUsage, subjectAltName basicConstraints, nameConstraints, cRLDistributionPoints</p> <p><u>Supported CRL extensions:</u> cRLNumber, reasonCode, invalidityDate, deltaInfo, issuingDistributionPoint, deltaCRLIndicator</p>	
<p>If the subjectAltName certificate extension is supported, which name types (from GeneralNames ASN.1 type) are supported?</p>	<p><b>m – x400Address (ORAddress), directoryName (Name)</b> <b>o – all other types</b></p>	

*c: if (strong authentication or signed operations) then m, else n/a*

### C.3.5 Requirements Statement for DSAs

**[AMHS-CA-C05]** Implementers shall state whether all of the requirements and which of the optional elements of the DSA supporting the Extended ATSMHS, as specified in ICAO Doc 9880 Part IVA [7] section 5, have been implemented, using the table in this section or equivalent.

*Note: The following table is derived from the X.500 conformance specifications taken from section 13.2.1 of ISO/IEC 9594-5 | ITU-T Rec. X.519 (2005) [34].*

**Table C-10: Directory System Agent Requirements**

X.500 Conformance Statement Requirements	initial Directory service	future Directory service
a) The application-contexts for which conformance is claimed: <b>directoryAccessAC</b> , <b>directorySystemAC</b> , <b>directoryOperationalBindingManagementAC</b>	<b>m - directoryAccessAC</b>	<b>m - directoryAccessAC</b> <b>directorySystemAC</b>
b) The operational binding types for which conformance is claimed: <b>shadowOperationalBindingID</b> , <b>specificHierarchicalBindingID</b> , <b>non-specificHierarchicalBindingID</b> , or a combination of these. A DSA that claims conformance to the shadowOperationalBindingID shall support one or more of the application contexts for shadow suppliers and/or shadow consumers	o	<b>o - shadowOperationalBindingID</b> should be supported
c) Whether or not the DSA is capable of acting as a first level DSA, as defined in ITU-T Rec. X.518   ISO/IEC 9594-4.	<b>m - Can act as first level DSA</b>	<b>m - Can act as first level DSA</b>
d) If conformance is claimed to the application-context specified by <b>directorySystemAC</b> , whether or not the chained mode of operation is supported, as defined in ITU-T Rec. X.518   ISO/IEC 9594-4.	-	<b>m - Chained mode shall be supported</b>
e) If conformance is claimed to the application-context specified by <b>directoryAccessAC</b> protocol, the bind security level(s) for which conformance is claimed (none, simple, strong – and if simple, then whether without password, with password, or with protected password); whether the DSA can perform originator authentication as defined in 22.1 of ITU-T Rec. X.518   ISO/IEC 9594-4 and if so, whether identity-based or signature-based; and whether the DSA can perform result authentication as defined in 22.2 of ITU-T Rec. X.518   ISO/IEC 9594-4.	<b>m – simple, with password</b>  o – Originator and Result authentication	<b>m – simple, with password</b>  o – Originator and Result authentication
f) If conformance is claimed to the application-context specified by <b>directorySystemAC</b> , the bind security level(s) for which conformance is claimed (none, simple, strong – and if simple, then whether without password, with password, or with protected password); whether the DSA can perform originator authentication as defined in 22.1 of ITU-T Rec. X.518   ISO/IEC 9594-4 and if so, whether identity-based or signature-based; and whether the DSA can perform result authentication as defined in 22.2 of ITU-T Rec. X.518   ISO/IEC 9594-4.	-	<b>m – simple, with password</b>  o – Originator and Result authentication
g) The selected attribute types defined in ITU-T Rec. X.520   ISO/IEC 9594-6: <u>System attribute types</u> Knowledge Information <u>Labelling attribute types</u> Name Common Name Surname Given Name Initials Generation Qualifier Unique Identifier DN Qualifier Serial Number Pseudonym Universal Unique Identifier Pair	<b>o – uUIDPair, all “Notification” attributes</b>  <b>m - all attributes defined in section C.3.2</b>	<b>o – uUIDPair, all “Notification” attributes</b>  <b>m - all attributes defined in section C.3.2</b>

EUROCONTROL SPECIFICATION  
on the  
Air Traffic Services Message Handling System (AMHS)

X.500 Conformance Statement Requirements	initial Directory service	future Directory service
<p><u>Geographical Attribute Types</u> Country Name Locality Name State or Province Name Street Address House Identifier</p> <p><u>Organizational attribute types</u> Organization Name Organizational Unit Name Title</p> <p><u>Explanatory attribute types</u> Description Search Guide Enhanced Search Guide Business Category</p> <p><u>Postal Addressing attribute types</u> Postal Address Postal Code Post Office Box Physical Delivery Office Name</p> <p><u>Telecommunications Addressing attribute types</u> Telephone Number Telex Number Teletex Terminal Identifier Facsimile Telephone Number X.121 Address International ISDN Number Registered Address Destination Indicator Communications Service Communications Network</p> <p><u>Preferences attribute types</u> Preferred Delivery Method</p> <p><u>OSI Application attribute types</u> Presentation Address Supported Application Context Protocol Information</p> <p><u>Relational attribute types</u> Distinguished Name Member Unique Member Owner Role Occupant See Also</p> <p><u>Domain attribute types</u> DMD Name</p> <p><u>Notification attributes</u> DSA Problem Search Service Problem Service-type Attribute Type List Matching Rule List Filter Item Attribute Combinations Context Type List Context List Context Combinations Hierarchy Select List Search Control Options List Service Control Options List Multiple Matching Localities Proposed Relaxation Applied Relaxation</p>		



EUROCONTROL SPECIFICATION  
on the  
Air Traffic Services Message Handling System (AMHS)

X.500 Conformance Statement Requirements	initial Directory service	future Directory service
Any other attribute types, for which conformance is claimed. For attributes based on the syntax <b>DirectoryString</b> , is conformance claimed for the <b>UniversalString</b> , <b>BMPString</b> , or <b>UTF8String</b> choices?		
h) The selected object classes defined in ITU-T Rec. X.521   ISO/IEC 9594-7: Country Locality Organization Organizational Unit Person Organizational Person Organizational Role Group of Names Group of Unique Names Residential Person Application Process Application Entity DSA Device Strong Authentication User User Security Information Certification Authority Certification Authority-V2 DMD Any other object classes, for which conformance is claimed.	<b>m</b> - all classes defined in section C.3.1	<b>m</b> - all classes defined in section C.3.1
i) The extensions listed in Table 1 of ITU-T Rec. X.511   ISO/IEC 9594-3, that the DSA is capable of responding to for which conformance is claimed.	o	o
j) Whether conformance is claimed for <b>collective attributes</b> as defined in 8.9 of ITU-T Rec. X.501   ISO/IEC 9594-2 and 7.6, 7.8.2 and 9.2.2 of ITU-T Rec. X.511   ISO/IEC 9594-3.	o	o
k) Whether conformance is claimed for <b>hierarchical attributes</b> as defined in 7.6, 7.8.2 and 9.2.2 of ITU-T Rec. X.511   ISO/IEC 9594-3	o	o
l) The operational attribute types defined in ITU-T Rec. X.501   ISO/IEC 9594-2 and any other operational attribute types for which conformance is claimed.	<b>o</b> - All operational attributes defined in ITU-T Rec. X.501   ISO/IEC 9594-2	<b>o</b> - All operational attributes defined in ITU-T Rec. X.501   ISO/IEC 9594-2
m) Whether conformance is claimed for return of <b>alias names</b> as described in 7.7.1 of ITU-T Rec. X.511   ISO/IEC 9594-3.	o	<b>m</b>
n) Whether conformance is claimed for indicating that returned entry information is complete, as described in 7.7.1 of ITU-T Rec. X.511   ISO/IEC 9594-3.	o	<b>m</b>
o) Whether conformance is claimed for modifying the object class attribute to add and/or remove values identifying auxiliary object classes, as described in 11.3.2 of ITU-T Rec. X.511   ISO/IEC 9594-3.	o	o
p) Basic Access Control. (ITU-T Rec. X.501   ISO/IEC 9594-2)	o	o
q) Simplified Access Control. (ITU-T Rec. X.501   ISO/IEC 9594-2)	o	o
r) Whether the DSA is capable of administering the subschema for its portion of the DIT, as defined in ITU-T Rec. X.501   ISO/IEC 9594-2. Note – The capability to administer a subschema shall not be divided; specifically, the capability to administer particular subschema definitions shall not be claimed.	o	o
s) The selected name bindings defined in ITU-T Rec. X.521   ISO/IEC 9594-7 and any other name bindings, for which conformance is claimed.	o	o
t) Whether the DSA is capable of administering collective attributes, as defined in ITU-T Rec. X.501   ISO/IEC 9594-2.	o	o
u) The selected context types defined in ITU-T Rec. X.520   ISO/IEC 9594-6, and any other context types, for which conformance is claimed.	o	o

EUROCONTROL SPECIFICATION  
on the  
Air Traffic Services Message Handling System (AMHS)

X.500 Conformance Statement Requirements	initial Directory service	future Directory service
v) Whether conformance is claimed for <b>contexts</b> as defined in 8.8, 8.9 and 12.8 of ITU-T Rec. X.501   ISO/IEC 9594-2, and in 7.3 and 7.6 of ITU-T Rec. X.511   ISO/IEC 9594-3.	o	o
w) Whether conformance is claimed for the use of contexts in RDNs, as defined in 8.5 and 9.3 of ITU-T Rec. X.501   ISO/IEC 9594-2, 7.7 of ITU-T Rec. X.511   ISO/IEC 9594-3, and ITU-T Rec. X.518   ISO/IEC 9594-4.	o	o
x) Whether conformance is claimed for the management of the DSA Information Tree, as defined in 7.13 of ITU-T Rec. X.511   ISO/IEC 9594-3.	o	o
y) Whether conformance is claimed for the use of <b>systems management</b> for administration of the Directory, as defined in ITU-T Rec. X.530   ISO/IEC 9594-10.	o	o
z) The selected managed objects and management attribute types defined in ITU-T Rec. X.530   ISO/IEC 9594-10, and any other managed objects and attributes, for which conformance is claimed.	o	o
aa) Rule-based Access Control. (ITU-T Rec. X.501   ISO/IEC 9594-2) Note – The support of security labels requires the following minimal support of contexts: Context lists as per 8.8 of ITU-T Rec. X.501   ISO/IEC 9594-2 and returnContexts per 7.6 of ITU-T Rec. X.511   ISO/IEC 9594-3.	o	o
bb) Whether conformance is claimed to integrity of Directory operations.	o	o
cc) Whether conformance is claimed that the DSA can hold and provide access to encrypted and digitally signed information.	o	o
dd) If conformance is claimed for strong authentication, signed operations, or protected operations, identification of the Certificate and CRL extensions for which conformance is claimed.	<p><b>c –</b> <u>Supported certificate extensions:</u> keyUsage, subjectAltName (see Note 1 above) basicConstraints, nameConstraints, cRLDistributionPoints</p> <p><u>Supported CRL extensions:</u> cRLNumber, reasonCode, invalidityDate, deltaInfo, issuingDistributionPoint, deltaCRLIndicator</p>	<p><b>c –</b> <u>Supported certificate extensions:</u> keyUsage, subjectAltName (see Note 1 above) basicConstraints, nameConstraints, cRLDistributionPoints</p> <p><u>Supported CRL extensions:</u> cRLNumber, reasonCode, invalidityDate, deltaInfo, issuingDistributionPoint, deltaCRLIndicator</p>

### C.3.6 Requirements Statement for Conformance by a Shadow Supplier

**[AMHS-CA-C06]** For a DSA supporting the directory information shadowing protocol, implementers shall state whether all of the requirements and which of the optional elements of the DSA supporting the Extended ATSMHS, as specified in ICAO Doc 9880 Part IVA [7] section 5.5, have been implemented, using the table in this section or equivalent.

*Note: The following table is derived from the X.500 conformance specifications taken from section 13.3.1 of ISO/IEC 9594-5 | ITU-T Rec. X.519 (2005) [34]. It is conditional upon DISP being supported.*

**Table C-11: Shadow Supplier Requirements**

X.500 Conformance Statement Requirements	initial Directory service	future Directory service
<p>a) The application context(s) for which conformance is claimed as a shadow supplier:  <b>shadowSupplierInitiatedAC,</b>  <b>shadowConsumerInitiatedAC,</b>  <b>shadowSupplierInitiatedAsynchronousAC,</b>  <b>shadowConsumerInitiatedAsynchronousAC.</b></p> <p>A DSA implementation claiming conformance as a shadow supplier and not supporting disp-ip shall, at a minimum, support either the shadowSupplierInitiatedAC or the shadowConsumerInitiatedAC. If the DSA supports the shadowSupplierInitiatedAC, it may optionally support the shadowSupplierInitiatedAsynchronousAC. If the DSA supports the shadowConsumerInitiatedAC, it may optionally support the shadowConsumerInitiatedAsynchronousAC. If claiming conformance to disp-ip, it shall be stated whether the implementation is capable of invoking the requestShadowUpdate operation, responding to a coordinateShadowUpdate, or both.</p>	n/a	<p><b>c1</b> – at least <b>shadowSupplierInitiatedAC</b> and <b>shadowConsumerInitiatedAC</b> shall be supported</p>
<p>b) The security-level(s) for which conformance is claimed (none, simple, strong).</p>	n/a	<p><b>c1</b> – None and simple  <b>c2</b> - strong</p>
<p>c) To which degree the UnitOfReplication is supported. Specifically, which (if any) of the following optional features are supported:</p>	-	-
– entry filtering on objectClass;	n/a	<b>c1</b>
– selection/Exclusion of attributes via AttributeSelection;	n/a	<b>c1</b>
– the inclusion of subordinate knowledge in the replicated area;	n/a	<b>c1</b>
– the inclusion of extended knowledge in addition to subordinate knowledge;	n/a	<b>c1</b>
– selection/Exclusion of attribute values based on contexts.	n/a	c2

c1: if DISP supported then m, else n/a

c2: if DISP supported then o, else n/a

### C.3.7 Requirements Statement for Conformance by a Shadow Consumer

**[AMHS-CA-C07]** For a DSA supporting the directory information shadowing protocol, implementers shall state whether all of the requirements and which of the optional elements of the DSA supporting the Extended ATSMHS, as specified in ICAO Doc 9880 Part IVA [7] section 5.5, have been implemented, using the table in this section or equivalent.

*Note: The following table is derived from the X.500 conformance specifications taken from section 13.4.1 of ISO/IEC 9594-5 | ITU-T Rec. X.519 (2005) [34]. It is conditional upon DISP being supported.*

**Table C-12: Shadow Consumer Requirements**

X.500 Conformance Statement Requirements	initial Directory service	future Directory service
<p>a) The application context(s) for which conformance is claimed as a shadow consumer:  <b>shadowSupplierInitiatedAC,</b>  <b>shadowConsumerInitiatedAC,</b>  <b>shadowSupplierInitiatedAsynchronousAC,</b>  <b>shadowConsumerInitiatedAsynchronousAC.</b></p> <p>A DSA implementation claiming conformance as a shadow consumer and not supporting disp-ip shall, at a minimum, support either the shadowSupplierInitiatedAC or the shadowConsumerInitiatedAC. If the DSA supports the shadowSupplierInitiatedAC, it may optionally support the shadowSupplierInitiatedAsynchronousAC. If the DSA supports the shadowConsumerInitiatedAC it may optionally support the shadowConsumerInitiatedAsynchronousAC. If claiming conformance to disp-ip, it shall be stated whether the implementation is capable of responding to the requestShadowUpdate operation, requesting a coordinateShadowUpdate, or both;</p>	n/a	<p>c1 – at least <b>shadowSupplierInitiatedAC</b> and <b>shadowConsumerInitiatedAC</b> shall be supported</p>
<p>b) The security-level(s) for which conformance is claimed            none,            simple,            strong</p>	n/a	<p><b>c1</b> - None, simple  <b>c2</b> - strong</p>
<p>c) Whether the DSA can act as a secondary shadow supplier (i.e., participate in secondary shadowing as an intermediate DSA);</p>	n/a	c2
<p>d) Whether the DSA supports shadowing of overlapping units of replication</p>	n/a	c2

c1: if DISP supported then m, else n/a

c2: if DISP supported then o, else n/a

**EUROCONTROL SPECIFICATION  
on the  
Air Traffic Services Message  
Handling System (AMHS)  
ANNEX D - Security**

**SPECIFICATION DOCUMENT IDENTIFIER: EUROCONTROL-SPEC-0136**

<b>Edition Number</b>	<b>:</b>	<b>2.0</b>
<b>Edition Date</b>	<b>:</b>	<b>18/09/2009</b>
<b>Status</b>	<b>:</b>	<b>Released</b>
<b>Intended for</b>	<b>:</b>	<b>General Public</b>
<b>Category</b>	<b>:</b>	<b>EUROCONTROL Specification</b>

## DOCUMENT CHANGE RECORD

The following table records the complete history of the successive editions of the present document.

EDITION NUMBER	EDITION DATE	INFOCENTRE REFERENCE	REASON FOR CHANGE	PAGES AFFECTED
0.1	16/01/08		Initial outline	All
0.2	25/01/08		Detail added	All
0.3	26/02/08		Further evolution. Input to Drafting Group	All
0.4	01/04/08		Further evolution. Comments from drafting group 29/02/08.	All
0.5	13/06/08		Draft for Review Group	All
0.6	24/10/08		Updated after informal stakeholder review. Was previously Annex C.	All
1.0	08/12/08		Updated after informal stakeholder review. Input to formal consultation.	All
1.1	27/07/09		Updated after ENPRM-01/2009 formal consultation.	All
2.0	18/09/09		Released Issue	Footers

## CONTENTS

<b>ANNEX D - SECURITY REQUIREMENTS .....</b>	<b>1</b>
<b>D.1. CONFIGURATION CONTROL .....</b>	<b>1</b>
D.1.1 MOC Element Identification .....	1
D.1.2 MOC Element Change Record .....	1
D.1.3 MOC Element Traceability Towards Regulatory Provisions .....	1
D.1.4 MOC Element Traceability towards International Standards .....	1
<b>D.2. REQUIREMENTS AND EXPLANATORY MATERIALS .....</b>	<b>2</b>
D.2.1 Introduction .....	2
D.2.2 General Requirements .....	2
D.2.2.1 Security Architecture .....	2
D.2.2.2 Cryptographic and Hashing functions .....	6
D.2.3 AMHS Security Specific Requirements.....	7
D.2.3.1 Security Policy .....	7
D.2.3.2 AMHS Security Framework .....	8
D.2.3.3 Recommendations for Secure Message Submission .....	9
D.2.3.4 Recommendations for Secure Message Reception .....	12
D.2.3.5 Message Sequence Integrity.....	14
<b>D.3. CONFORMITY ASSESSMENT MATERIALS .....</b>	<b>16</b>
<b>APPENDIX 1 TO ANNEX D - PDR Resolutions Applicable to ICAO Doc 9705, Third Edition, Sub-Volume VIII.....</b>	<b>17</b>





## ANNEX D – SECURITY REQUIREMENTS

### D.1. CONFIGURATION CONTROL

#### D.1.1 MOC Element Identification

MOC_Name	MOC_Version	MOC_Edition
AMHS_SEC	1	1

#### D.1.2 MOC Element Change Record

The following table records the complete history of the successive editions of MOC specifications.

Version Number	Edition Number	Edition Date	Reason for Change	Sections Affected
1	1	18/09/09	Initial specification	All

#### D.1.3 MOC Element Traceability Towards Regulatory Provisions

The following table records the traceability history of regulatory provisions associated with this MOC element.

Version Number	Edition Number	Implementing rule references	References of regulatory provisions	Validation date
1	1	N/A	Regulation (EC) No 552/2004 [1] Annex II Part A and Part B (4) - Essential requirements applicable to communications systems and procedures for ground-to-ground communications	22/10/08

#### D.1.4 MOC Element Traceability towards International Standards

The following table records the traceability of international standards associated with this MOC element.

International standards identification	References of text parts used to draft MOC specifications	References of text parts imported into the MOC
ICAO Doc 9880 Part IIB [5]		Functional Group SEC
ICAO Doc 9705 Sub-Volume VIII [6]		ECDSA and related algorithms, PKI

## D.2. REQUIREMENTS AND EXPLANATORY MATERIALS

### D.2.1 Introduction

*Note 1: This informative Annex is included for guidance to potential implementers of the technical security features of the Extended ATSMHS.*

*Note 2: This Annex aims to provide complementary information for the EATMN on the application of security aspects defined in the ICAO technical specifications for ATN Security [6]. Any differences or complementary specifications with respect to the ICAO provisions are explicitly identified.*

*Note 3: The first part of the Annex (D.2.2) deals with general security framework requirements, while the second part (D.2.3) deals with security requirements specific to AMHS.*

*Note 4: This Annex must be read in conjunction with the Main Body of this EUROCONTROL Specification, which provides definitions, document references and contextual information. References given in square brackets are defined in section 10 of the Main Body. Reference is also made to Annex C of this EUROCONTROL Specification for the definition of the Directory system supporting certificate and CRL distribution.*

*Note 5: Due to the informative nature of this Annex, the use of “shall” and “should” to identify requirements and recommendations differs from their usage in the other Annexes of this EUROCONTROL Specification. The respective requirements and recommendations are applicable only in cases where it is decided to include AMHS message security in a particular implementation.*

### D.2.2 General Requirements

*Note: The technical provisions specified in this Annex will be just one element of an overall security framework that would be necessary to protect the assets of the AMHS and its users from malicious attack. Other technical elements include virus protection, firewalls, etc.*

#### D.2.2.1 Security Architecture

*Note: ANSPs will need to provide further specifications for any purely local protocol aspects that remain options in the ISPs e.g. the details of UA-MTA and UA-MS Bind Operations and Authentication resulting from an ANSP’s local security policy.*

**[AMHS-SEC-D01]** An AMHS End System implementation shall implement protocol provisions as necessary to comply with the local security policy relating to aeronautical data access and interchange.

*Note: A minimum set of compliance requirements for such protocol provisions is specified in this EUROCONTROL Specification.*

**[AMHS-SEC-D02]** Measures should be taken by ANSPs and other entities providing data communications services to ensure appropriate security of information exchanges

**[AMHS-SEC-D04]** Implementations shall be conformant with the Extended ATSMHS and in particular the security aspects of ATN relevant for ground-ground communication; Chapter 8.3.1.1 (Framework Standards) of the ATN Security provisions [6] is fully applicable.

**[AMHS-SEC-D05]** Each State implementing AMHS Security shall designate a Trusted Third Party (TTP) acting as a Root Certificate Authority (CA) which issues certificates and certificate revocation lists (CRLs), in accordance with chapter 8.3.1.2.2 of the ATN Security provisions [6].

*Note 1: Due to geopolitical, governance and local policies aspects, it is important that each State is free to select a CA of their choice. This CA can be public or private. Several States / Organisations may decide to share the same CA.*

*Note 2: The CA chosen by the State must comply with local laws and regulations.*

**[AMHS-SEC-D06]** The TTP shall conform to the ETSI Guide EG 201 057 [13], which defines the role and attribution of a TTP acting as a CA in a PKI.

**[AMHS-SEC-D07]** Item 8.3.1.2.3 of the ATN Security provisions [6] shall be applicable in the conditions provided below.

*Note: The referenced item states that State CAs shall have a non-transitive peer relationship among one another, rather than a hierarchical relationship. To ensure that relationships can be defined globally with countries conformant to the ATN provisions, the policies used in Europe can be applied as-is by the other countries.*

**[AMHS-SEC-D08]** CAs in the EATMN shall use policies to ensure the overall security of the ATN.

**[AMHS-SEC-D09]** CAs shall be conformant with Directive 1999/93/EC [2], which defines a Community framework for electronic signatures.

**[AMHS-SEC-D10]** CAs shall comply with the certificate policy requirements defined in ETSI specification TS 101 456 [14].

*Note 1: The referenced ETSI specification is conformant with European directive 1999/93/EC. According to ETSI TR 102 040 [32], this specification has been defined to help cross certification between CAs over the world.*

*Note 2: The policy defined in TS 101 456 [14] is defined with respect to guidelines given in PAG (PKI Assessment Guidelines v0.30 edited by the American Bar Association) and RFC 3647 [21] – Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework.*

**[AMHS-SEC-D11]** Where the ATN Security provisions [6] in section 8.4 refer to RFC 2527, this shall be replaced with a reference to RFC 3647 [21].

**[AMHS-SEC-D12]** CAs shall develop a Certificate Policy (CP) that defines the creation, management, and use of public key certificates that they issue, consistent with section 8.4.1.1 of the ATN Security provisions [6].

**[AMHS-SEC-D13]** CAs shall publish a Certificate Practice Statement (CPS) that describes the expected use of public key certificates that they issue, consistent with section 8.4.2.1 of the ATN Security provisions [6].

*Note: Practices may include such items as initialisation/certification of entities and their key pairs, certificate revocation, key backup and recovery, CA key rollover, cross-certification, etc.*

**[AMHS-SEC-D14]** The CP and CPS shall be aligned with the framework presented in RFC 3647 [21].

*Note 1: The above reference differs from sections 8.4.1.2 and 8.4.2.2 of the ATN Security provisions [6], which require that “the Certificate Policy and Certificate Practice Statement shall conform to the Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, IETF PKIX RFC2527”. RFC 2527 is obsoleted by RFC 3647.*

*Note 2: The CP and CPS of a given State could be used by other States in establishing their trust relationships and operating policies such as cross certification.*

**[AMHS-SEC-D15]** Each CA shall define its own CPS conformant with the rules defined in ETSI TS 101 456 [14].

**[AMHS-SEC-D16]** Each CA shall propose a service for certificate and CRL distribution.

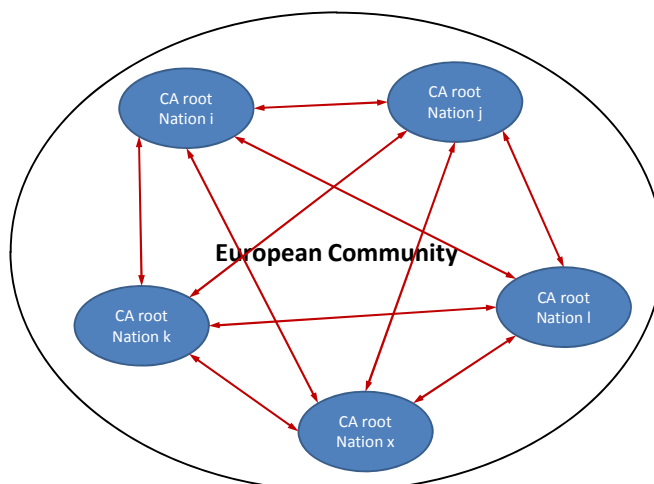
**[AMHS-SEC-D17]** Each CA shall give simple access to the public certificate and CRL repository in its own domain.

**[AMHS-SEC-D18]** The distribution system of public key certificates and CRLs should be done using Directory services.

**[AMHS-SEC-D19]** According to item 8.3.1.2.7 of the ATN Security provisions [6]: “If a directory service is used for certificate and CRL distribution, the service shall conform to the ATN directory service as specified in [...ICAO Doc 9880 Part IVA [7]]”. This shall be taken to mean conformity with the Directory as specified in Annex C of this EUROCONTROL Specification.

#### **D.2.2.1.1 PKI Deployment in the EATMN**

*Note: If it were to evolve in an uncoordinated manner, there is a risk that the PKI implementation for EATMN ground-ground communication could result in the architecture presented in Figure D-1, where each State has a bilateral cross-certification with all other participating States (so for N participants, it implies  $N(N-1)$  relations of confidence need to be put in place). For example, if 10 States were to interconnect together, a total of  $10*9 = 90$  bilateral cross-certifications are required.*



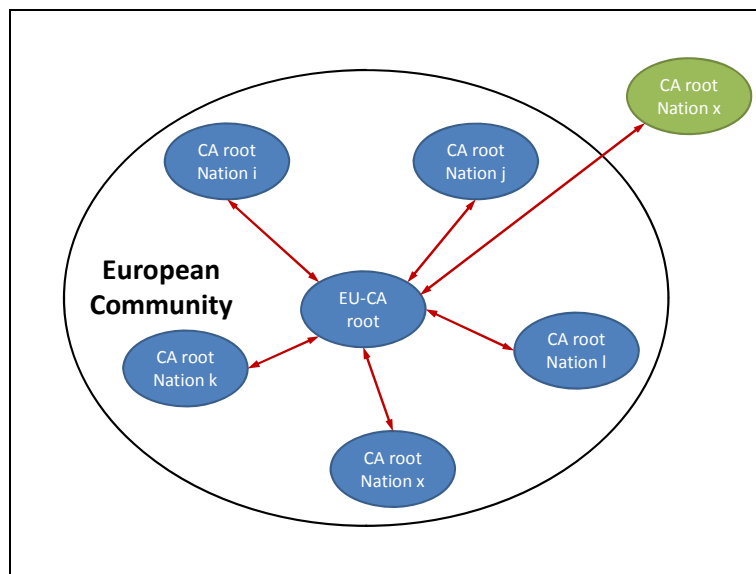
**Figure D-1: European PKI with Multiple Cross-Certified CAs**

*In this infrastructure, all participating States would have to conform to a common security policy.*

**[AMHS-SEC-D20]** The EATMN PKI in support of AMHS should therefore be based on a common ATS Bridge CA (see Figure D-2) in order to:

- a) Simplify the process of cross-certification for each CA;
- b) Minimise the issues due to multiple policy agreements;
- c) Minimise the risk of problems occurring due to the limit of validity of cross certificates;
- d) Allow a central organisation to verify that the policy applied by each CA complies with the European directive on a Community framework for electronic signatures [2].

*Note 1: In this case, and only in this case, a transitive relationship may be allowed between two States' CAs if a central EATMN-wide CA Root is provided.*



**Figure D-2: Future European Public Key Infrastructure**

*Note 2: Due to a number of considerations, it is unlikely that the common European ATS Bridge CA with all State CAs participating as envisaged above will be available in a single step. As an initial transition step, it may be possible to establish a single central CA as a common facility, with ANSPs using certificates issued by this CA rather than by their National CA for message signatures. More practically, their CAs could be subCAs of the single central CA, otherwise there could be significant time delays when adding or removing users.*

#### **D.2.2.2 Cryptographic and Hashing functions**

*Note: In order to achieve interoperability across the EATMN and beyond, it is necessary that each implementation of the Extended ATSMHS uses a common set of algorithms and parameter settings for cryptographic and hashing functions.*

**[AMHS-SEC-D21]** The cryptographic signing and hashing functions and parameter settings shall be conformant with ATN Security provisions [6], Chapter 8.5.

*Note 1: The detailed technical specifications for ATN Security [6] specify the use of an Elliptic Curve cryptosystem for ATN public-key algorithms. Cryptographic and Hashing functions defined in the ATN Security provisions are conformant with ETSI recommendation TS 102 176-1 [33].*

*Note 2: The maintenance procedures for this EUROCONTROL Specification allow the possibility of updating the choice of security algorithms and associated parameters used for digital signatures and public key authentication. For example, an upgrade to conform to current NIST security suites could be foreseen.*

**[AMHS-SEC-D22]** The general certificate format used for ATN PKI certificates shall be conformant with the X.509 Format with parameters defined in chapter 8.4.3 of the ATN Security provisions [6].

**[AMHS-SEC-D23]** The signature scheme E-ATSMHS-SEC shall be conformant, for the hash function, to the Secure Hash Standard (SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512) defined in FIPS 180-2: Secure Hash Standard (SHS) [15].

*Note: The content integrity check algorithm is based on the E-ATSMHS-SEC signature scheme ("ecdsa-with-SHA2"). The signature scheme ("ecdsa-with-SHA2") is drawn from the ATN signature scheme ("ecdsa-with-SHA1") and consists of replacing the SHA-1 hash function with one of the SHA-2 family function: SHA-224, SHA-256, SHA-384, and SHA-512.*

**[AMHS-SEC-D24]** The elements of a certificate should be encoded following the DER (Distinguished Encoding Rules) standard defined in the ITU-T Rec X.509 [35] (section 8.7) and specified by the ITU-T Rec X.690 [36].

**[AMHS-SEC-D25]** It is recommended that a symmetric algorithm should be used for the Content Integrity Check algorithm in Extended ATSMHS, and that this should initially be the secure hash algorithm "SHA-1".

*Note: SHA-1 is being replaced with stronger algorithms such as "SHA-256", but this may not be necessary for ATS messages; depending on the threat model.*

## **D.2.3 AMHS Security Specific Requirements**

### **D.2.3.1 Security Policy**

**[AMHS-SEC-D26]** If secure messaging is required in the Extended ATSMHS, a general AMHS end-to-end security policy shall be implemented in compliance with ICAO Doc 9880 Part IIB [5] section 2.2.3, providing the following security services:

- a) Message origin authentication; and
- b) Content integrity.

*Note: ICAO Doc 9880 Part IIB also specifies Message Sequence Integrity as a provided service. See D.2.3.5 below.*

**[AMHS-SEC-D27]** An appropriate security policy shall be implemented in order to secure the AMHS, notably by applying common security rules to protect the distributed physical resources supporting message submission, transfer and delivery.

*Note 1: Definition of a security policy is beyond the scope of this EUROCONTROL Specification. Such a policy will comply with the requirements various international standards, including ICAO Annex 17 [29], ICAO EUR Security Guidelines [10], and Regulation (EC) 2096/2005 [25].*

*Note 2: The security policy for EATMN ground-ground communication also needs to consider communication with external countries, and not impose security elements that will prevent communication where such communication is required.*

**[AMHS-SEC-D28]** For messages using these security services, the processing of the message envelope shall be in compliance with ICAO Doc 9880 Part IIB [5] sections 3.1.4.3 and 3.2.4.

*Note: This requires support of security class S0 as defined in section 7 of ISP 10611-1 [19].*

### **D.2.3.2 AMHS Security Framework**

*Note: This section first describes the security services provided to the different users (ATS Message User Agent, ATS Message Server, AFTN/AMHS Gateway) and then deals with security framework for AMHS such as end to end AMHS user message exchange security (PKI). It gives related normative documents from standards bodies such as ITU, ISO and IETF applicable in the context of AMHS.*

**[AMHS-SEC-D29]** The Security model given in §2.2.3 of the AMHS technical provisions in ICAO Doc 9880 Part IIB [5] shall be applied.

**[AMHS-SEC-D30]** The general AMHS security policy shall be aligned with the general ATN Security Framework as defined in the ATN Security provisions [6]; this is a common minimum which does not prevent specific communities of AMHS users from implementing more stringent security policies in case of additional user requirements.

**[AMHS-SEC-D31]** The use of AMHS security services shall apply to:

- a) communications between direct AMHS users supporting the Extended ATSMHS; and
- b) communications from direct AMHS users to indirect AMHS users as far as the AFTN/AMHS Gateway supporting the Extended ATSMHS.

*Note: ICAO Doc 9880 Part IIB [5] section 3.1.2.1.2.3.3 notes that it is only possible to perform asymmetric authentication of a direct AMHS user by an AFTN/AMHS Gateway.*

**[AMHS-SEC-D32]** The AMHS security policy shall make use of the Elliptic Curve Digital Signature Algorithm (ECDSA) as specified in the ATN Security provisions [6] section 8.5.5.

**[AMHS-SEC-D33]** For the support of security in the context of the Extended ATSMHS, an ATS Message User Agent shall implement the Security requirements defined in §3.1.4.3.2 of ICAO Doc 9880 Part IIB [5].

*Note: The specified cryptographic and hashing functions are used to generate and verify digital signatures for messages exchanged between ATS Message User Agents supporting AMHS Security.*

**[AMHS-SEC-D34]** The generation by the ATS Message User Agent of the message token in the per-recipient-extensions of the message envelope shall be as specified in section 3.1.4.3.2.2.1 of ICAO Doc 9880 Part IIB [5], refined as specified in this Annex.

**[AMHS-SEC-D35]** For the support of security in the context of the Extended ATSMHS, an MTA in an ATS Message Server shall implement the requirements for the support by an MTA of the SEC Functional Group, implementing Security-Class S0, as defined in §3.2.4.3 b) of ICAO Doc 9880 Part IIB [5].

**[AMHS-SEC-D36]** For the support of security in the context of the Extended ATSMHS, a Message Store in an ATS Message Server shall implement the requirements for the support by an MS of the SEC Functional Group, implementing Security-Class S0, as defined in §3.2.4.4 b) of ICAO Doc 9880 Part IIB [5].

**[AMHS-SEC-D37]** For the support of security in the context of the Extended ATSMHS, an AFTN/AMHS Gateway shall implement the requirements for handling the security-related



elements of the message transfer envelope as defined in §4.5.2.4.12 to 4.5.2.4.16 of ICAO Doc 9880 Part IIB [5].

*Note: The specified cryptographic and hashing functions may be used for messages addressed to indirect AMHS users if the AFTN/AMHS Gateway supports AMHS Security. Although not providing end-to-end security in this case, the security service can help to prevent unauthorised users from accessing the gateway, provided that the gateway knows which users are expected to sign messages.*

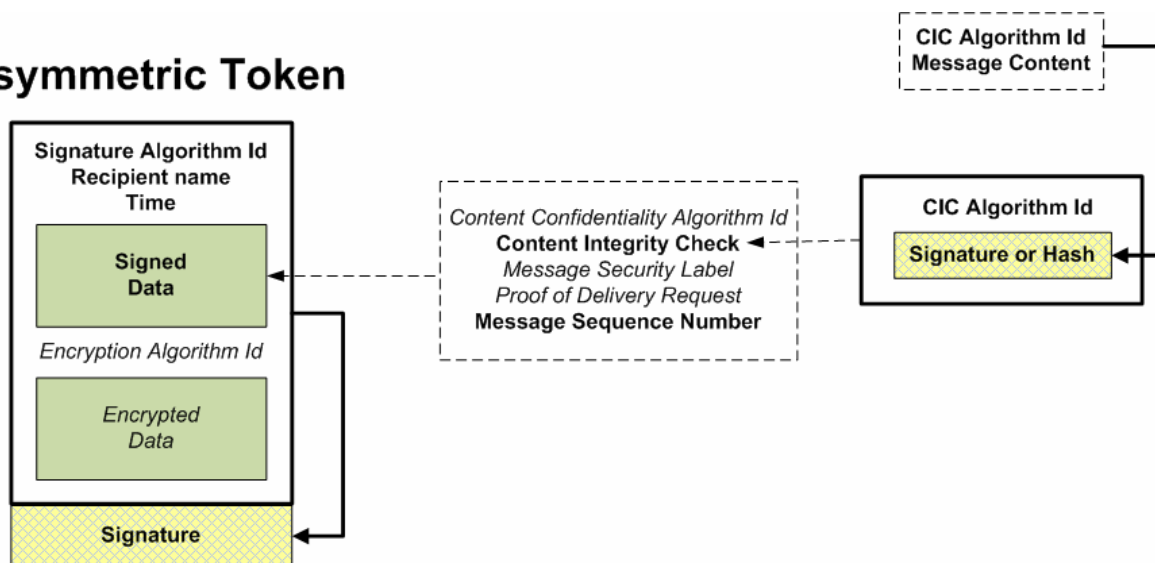
**[AMHS-SEC-D38]** It is recommended that to simplify certificate signature checking, and facilitate interoperability, the certificate (and CRL) extensions that may be used within the Extended ATSMHS are precisely defined and kept to a minimum.

### D.2.3.3 Recommendations for Secure Message Submission

#### D.2.3.3.1 Use of Message Token

*Note: A message-token is a general purpose structure for conveying signed (and possibly also encrypted) information from originator to recipients, in circumstances where some of the information needs to be specified differently per recipient. The message-token is depicted graphically in Figure D-3. (Items in italics are not used by AMHS Security).*

### Asymmetric Token



**Figure D-3: Content of Message Token**

**[AMHS-SEC-D39]** A message originator wishing to send a secure message at an ATS Message User Agent that supports AMHS SEC shall create and sign a message-token for each recipient in the per-recipient-extensions in the message envelope.

*Note: The AsymmetricToken form of the message-token is used by AMHS Security, as shown in Figure D-4. The SIGNED construct indicates that the SEQUENCE construct is present in plaintext, followed by a signature appendix.*

```

SIGNED { ToBe Signed } ::= SEQUENCE{
  toBe Signed      ToBe Signed,
  COMPONENTS OF   SIGNATURE { ToBe Signed }
}
AsymmetricToken ::=
  SIGNED
  {SEQUENCE {signature-algorithm-identifier AlgorithmIdentifier,
    name
      CHOICE {recipient-name RecipientName,
        mta
          [3] SEQUENCE {global-domain-identifier
            GlobalDomainIdentifier OPTIONAL,
              mta-name MTAName
            }},
        time Time,
        signed-data [0] TokenData OPTIONAL,
        encryption-algorithm-identifier
          [1] AlgorithmIdentifier OPTIONAL,
        encrypted-data
          [2] ENCRYPTED{TokenData} OPTIONAL}}

```

**Figure D-4: ASN.1 definition of Message Token**

The *AsymmetricToken* includes:

- a) A signature algorithm identifier, which for AMHS Security is the value "ecdsa-with-SHA1" with NULL parameters;
- b) A name. For AMHS Security this would be the O/R Name of the recipient. It typically matches the recipient O/R Name to which it refers, but this is not the case after distribution list expansion or when the message has been redirected;
- c) The time the message-token was created;
- d) Signed data information, as shown in Figure D-5.
- e) Encryption algorithm identifier. Not used for AMHS Security.
- f) Encrypted data. Not used for AMHS Security.

```

MessageTokenSignedData ::= SEQUENCE {
  content-confidentiality-algorithm-identifier
    [0] ContentConfidentialityAlgorithmIdentifier OPTIONAL,
  content-integrity-check
    [1] ContentIntegrityCheck OPTIONAL,
  message-security-label
    [2] MessageSecurityLabel OPTIONAL,
  proof-of-delivery-request
    [3] ProofOfDeliveryRequest OPTIONAL,
  message-sequence-number
    [4] INTEGER OPTIONAL
}

```

**Figure D-5: ASN.1 definition of Signed Data information**

Of the various elements of the signed data information, the AMHS SEC only uses the Content Integrity Check (CIC). This consists of the algorithm identification followed by a computed integrity-check value, as shown in Figure D-6. The SIGNATURE construct for the

CIC indicates that the algorithm is applied to both the algorithm identifier and the message content. It is possible to use an asymmetric algorithm (e.g. "ecdsa-with-SHA1") or a symmetric algorithm (e.g. "SHA-1"). The symmetric algorithm is recommended because it is quicker to compute. Note that "SHA-1" is being replaced with stronger algorithms such as "SHA-256", but this may not be necessary for ATS messages, depending on the threat model.

```
SIGNATURE { ToBeSigned } ::= SEQUENCE {
  algorithmIdentifier AlgorithmIdentifier,
  encrypted           ENCRYPTED-HASH { ToBeSigned }}
ContentIntegrityCheck ::=
  SIGNATURE
  {SEQUENCE {algorithm-identifier
             ContentIntegrityAlgorithmIdentifier OPTIONAL,
             content Content}}
```

**Figure D-6: ASN.1 definition of Content Integrity Check**

[AMHS-SEC-D40] The MessageTokenSignedData should include only the CIC algorithm identifier and the CIC value, computed using a symmetric algorithm.

#### **D.2.3.3.2 Inclusion of originator's certificate**

*Note 1: In order to verify a message signature, a message recipient must obtain the correct public key of the message signer. This is held in the signer's certificate. When submitting a message, an AMHS user which supports AMHS SEC can optionally include the certificate containing their own public key within the message envelope.*

*Note 2: If no certificate is supplied by the message originator, the message recipient must look up the correct certificate in the directory. It is necessary for the receiving application to identify the directory entry of the message signer (preferably via a Directory Name (DN) in the originator's O/R Name, otherwise by a directory search for the originator's O/R Address), then perform a directory lookup and download the certificate attribute, then pick out the correct certificate from the set of values in the certificate attribute. There can be several certificate values because certificate keys may be rolled over after a period of time (say, 1 year) but the old values need to be retained to (partially) verify signatures of old messages. The application needs to select a certificate value with a validity period matching the message submission/delivery time, even if the validity period has expired. This approach is not recommended because of the extra time it will take to verify a signature, and the extra load placed on the directory.*

*Note 3: There are various approaches for including the originator's certificate with the message, including:*

- a) *Originator provides certificate in message envelope*

*This is by far the most common approach adopted, and it is strongly recommended that this approach is followed in ATS Message User Agents that support SEC. The message originator places the certificate containing the required public key in the **originators-certificate** element in the message envelope extensions.*

*The advantage of this approach is that recipients are provided with exactly the right certificate to proceed with signature verification. There is no need to identify the directory entry of the message signer, then perform a directory lookup and download the certificate attribute, then pick out the correct*

*certificate from the set of values in the certificate attribute. All of these operations introduce processing delays.*

*Note that with this approach, users' certificates don't need to be published to the directory at all. This simplifies maintenance and makes replication between different directories simpler.*

*Also note that when the certificate is stored with the message, it can be used to perform an integrity check on an archived message, after the certificate validity period has expired and non-repudiation of origin is no longer practical.*

*The only disadvantage is that messages are bigger than necessary because of the certificate, which might be around 1 kByte in size.*

- b) *Originator provides certificate in **multiple-originator-certificates** element of message*

*In this approach, the message originator places one or more certificates in the **multiple-originator-certificates** element in the message envelope extensions. This field is currently available for use in the Extended ATSMHS profile, but there is no reason to use it, as all message recipients will be capable of using the same originator's certificate.*

**[AMHS-SEC-D41]** It is recommended that message originators using AMHS Security should provide a valid certificate containing the required public key in the *originators-certificate* element in the message envelope extensions.

*Note: Providing the originator's certificate in the message envelope is optional, but is strongly recommended for Extended ATSMHS systems due to the reduced processing overheads.*

**[AMHS-SEC-D42]** It is recommended that use of the *multiple-originator-certificates* element in the message envelope extensions should be prohibited on message submission.

*Note: It should not be necessary to provide more than one certificate, as in Extended ATSMHS all message recipients will be capable of using the same originator's certificate.*

## **D.2.3.4 Recommendations for Secure Message Reception**

### **D.2.3.4.1 Certificate validation**

*Note: Upon receiving a signed message, an ATS Message User Agent which supports AMHS SEC must retrieve the originator's certificate and validate it. To validate a certificate, it is necessary to:*

- a) *Verify that the certificate is associated with the message originator;*
- 1) *One approach is to compare the DN provided in the originator's O/R Name with the Subject's Name in the certificate. This approach is not recommended as there may not be a DN in the originator's O/R Name.*
  - 2) *The recommended approach is to compare the originator's O/R Address with one found in the Subject Alternative Name extension of the certificate. This approach is much more flexible as the check is a pure X.400 check not involving the directory. The message originator must have access to the correct private key to sign the message. It is not relevant which entry in the directory (if any) is used to store the certificate, so the DIT structure of the originating and receiving organisations could be different.*

b) *Check that the certificate has not expired or been revoked, and has a valid signature*

1) *One option is for the recipient to use the Online Certificate Status Protocol (OCSP, RFC 2560 [41]). The certificate is passed to an OCSP Responder which validates it and returns the result. The OCSP Responder is a server component that can often perform directory lookups faster than a client application, which may need to make requests across a network.*

2) *Another option is for the application itself to check the certificate. This would involve the following operations:*

i. *Compare the validity period of the certificate with the current time. (This requires all EATMN systems to have their time synchronised to within a few minutes). Note that if the validity period has expired, this would be unacceptable to an AFTN/AMHS Gateway or ATS Message User Agent receiving a new message, but might be acceptable for an ATS Message User Agent displaying an archived message. If the validity period has expired for an archived message, the ATS Message User Agent can use the certificate to verify message integrity but not attempt a full signature check; it could inform the user that the full signature can no longer be checked.*

ii. *Check the certificate signature. The certificate will be signed by a CA, and to check the signature the CA's certificate must be obtained. This is to be found in the caCertificate attribute of a CA's directory entry. This certificate will be self-signed if this is the root CA; otherwise, a chain of CA certificates must be retrieved and checked back to the root CA. (Or if the originator and recipient do not share the same root CA, somewhere in the chain will be a cross-certificate attribute, possibly belonging to a Bridge CA, to be processed).*

iii. *Check for revocation. For each CA in the certificate path, a Certificate Revocation List (CRL) must be retrieved from the directory to check that none of the certificates it issued has since been revoked. The CRL itself has a signature which must be checked. A CA may delegate the issuing of CRLs to a CRL Issuer; if so, information explaining where to find the CRL needs to be provided in certificates.*

*Once the originator's certificate has been validated, the public key within it can be used to check the message signature.*

**[AMHS-SEC-D43]** *It is recommended that on receipt of a message containing the originator's certificate in the message envelope extensions, the originator's O/R Address should be compared with one found in the Subject Alternative Name extension of the certificate to ensure that the supplied certificate is associated with the message originator.*

**[AMHS-SEC-D44]** *It is recommended that an OCSP Responder compliant with RFC 2560 [41] should be deployed to facilitate the verification of received certificates.*

*Note: This approach has the advantage that the validation rules in the OCSP Responder can be adjusted and a standard validation algorithm will apply to all applications using it.*

#### **D.2.3.4.2 Message token processing**

**[AMHS-SEC-D45]** *An application should validate the message token, contained in the message delivery envelope extensions, when the message is first received, including:*

a) *Verifying the time field in the message token;*

- b) Applying the CIC Algorithm Id to the received message content / stated algorithm id, and comparing this to the received CIC Hash value;
- c) Applying the Signature Algorithm Id and originator's certificate public key to the whole contents of the Asymmetric Token, and comparing this with the token signature;
- d) Checking the Recipient Name in the message-token.

**[AMHS-SEC-D46]** A receiving application should report an error if a message-token that is 'too old' is received (except when displaying an archived message).

**[AMHS-SEC-D47]** The maximum acceptable time difference between the time field in the message token and the current system time should be specified in the security policy.

**[AMHS-SEC-D48]** If a message is received that is too old, the receiving application should check the message integrity but ignore the signature.

*Note: After a signed message has been received and validated, an ATS Message User Agent might want to re-use the message-token whenever the message is opened for display purposes. In such a situation, checking the message-token recipient name, time, and message sequence number is not valid. The ATS Message User Agent might automatically perform an integrity check using the CIC (as this does not involve the directory and so is very fast), but provide the user with an option to perform a full signature check on the message (which is likely to fail if the message is old).*

**[AMHS-SEC-D49]** When applying the CIC Algorithm Id to the received message content / stated algorithm id, and comparing this to the received CIC Hash, it is recommended that the AMHS SEC convention is to use the message content as received, i.e. the recipient should not need to ensure that it is DER-encoded.

*Note: The above recommendation assumes that the CIC Algorithm is symmetric; otherwise the process is more complicated. It improves performance, and is acceptable because ATS Message Servers never modify the message content en route, as they do not support the Conversion functional group.*

### **D.2.3.5 Message Sequence Integrity**

*Note 1: The Message Sequence Number in the Message Token may be set individually for each recipient. This would allow a recipient to detect replay, re-ordering, and message loss. Re-ordering may not be important for an ATS Message User Agent, but could be for a specialised application (e.g. receiving database updates to be applied in a particular sequence). Both the sending and receiving applications would need to keep track of what is the next expected number. However, it is recommended not to use the message sequence number field for message sequence integrity, since sequencing problems may be quite common:*

- a) *If the message originator is sending messages of different priority. An MTA will send high-priority messages first;*
- b) *If there are multiple channels between a pair of MTAs. In this situation, a small message may overtake a large message on another channel;*
- c) *If there are alternate routes between a pair of MTAs, involving other MTAs.*

*Note 2: Support for Message sequence integrity is indicated in ICAO Doc 9880 Part IIB [5], as a countermeasure against replay. The details of how to provide such a service are not defined. Message sequence assurance in an AFTN/AMHS Gateway may be provided by means of timestamp analysis. Use of the message sequence field in the Message Token is not required for compliance with this EUROCONTROL Specification (nor is it prohibited).*

**[AMHS-SEC-D50]** Message sequence integrity should be achieved by the message originator setting the Time field in the Message Token to the current time, and the message recipient checking that the value of this field is within acceptable parameters.

**[AMHS-SEC-D51]** Message sequence integrity may be provided as claimed in ISO/IEC 10021-4 [18]. In an AMHS End System supporting the Extended ATSMHS, the message-sequence-number may be present in the asymmetric token *MessageTokenSignedData*. As stated in ISO/IEC 10021-4 [18], the first occurrence of a message sequence number can be a random number.

**[AMHS-SEC-D52]** However, it is recommended that applications using the Extended ATSMHS should avoid using the message-sequence-number field in the Message Token for message sequence integrity assurance.

*Note: If the above recommendation is not followed, and message sequence integrity is important (e.g. not when just displaying a list of messages), the following initial check would have to be made before acting on the received sequence number. If the Recipient Name in the message-token matches the message delivery envelope this-recipient-name field, the receiving application is free to use the message sequence number provided in the message-token, as the message has not been redirected and there has been no DL expansion involving the recipient. Otherwise, the receiving application should not use any message sequence number provided in the message-token, because it was generated for another user (or for a distribution list).*

### **D.3. CONFORMITY ASSESSMENT MATERIALS**

D.3.1 This section specifies the Profile Requirements List (PRL) for the services specified in Annex D.

**[AMHS-CA-D01]** For ATS Message User Agent implementations supporting the SEC functional group, a PICS shall be provided stating the level of support, for each of the elements listed in the profile requirements list in Table 3-3 of ICAO Doc 9880 Part IIB [5].

**[AMHS-CA-D02]** Support for message-sequence-number in the message token signed-data, which is indicated as “Optional” in the referenced PRL, should be made “M” (Mandatory), to allow for the possible provision of the Message Sequence Integrity function.

**[AMHS-CA-D03]** Support for the encrypted-data and content-confidentiality-algorithm-id fields in the message token, which is indicated as “Optional” in the referenced PRL, should be considered “out of scope”, and not used when communicating with AMHS users compliant with this EUROCONTROL Specification, since the AMHS security model in ICAO Doc 9880 Part IIB [5], does not include message confidentiality.



## **APPENDIX 1 TO ANNEX D**

### **PDR Resolutions Applicable to ICAO Doc 9705, Third Edition, Sub-Volume VIII**

*Note: A number of Proposed Defect Reports (PDRs) applicable to the ATN Security service were considered and resolved by working groups of the ICAO ATN Panel. The PDR resolutions have been incorporated into the Draft ICAO Doc 9705 Edition 4, but this will not be published by ICAO; it will eventually be included in ICAO Doc 9880, Part IV.*

*Until the Security chapter of ICAO Doc 9880 Part IV becomes available, this Appendix will reference the applicable PDR resolutions, which can be found in the Repository section of the ICAO ACP website.*

**[AMHS-SEC-D54]** Security implementations shall include the relevant PDR resolutions from the following list:

<b>PDR ref</b>	<b>Title</b>
M1030007	Security - Editorial errors found during development of Guidance Material
M1030008	Security - Defects found during development of Guidance Material
M2030004	All SV - Editorials (version of PDR current on 2004/05/28)
M2080001	SV8 - Unnecessary random challenge field
M2080003	Security - Clarify representation of AMHS identities in ATN certificates
M2080004	Security - Additional extensions in CA certificates
M2080005	Security - Clarify ATN CRL processing
M2080006	Security - Add warning concerning the use of invalid keys by the secret value derivation primitive
M2080007	Security - Remove CheckResult references from 8.6.3
M2080008	Security - Remove duplicate certificate retrieval requirements
M2080009	Security - Sub-Volume VIII ASN.1
M2090002	SV8, SV4 - SSO-GetCertificatePath target
M2090003	SV8 - ASN.1 padding issues
M2090004	SV8 - SSO-SessionKey Certificate Knowledge
M2090005	SV8 - SSO counter initialization
M2100005	SV8 - Tagging in SV8 ASN.1 module
M4020001	Security - Error in ATN Key Derivation Function
M4030001	SV8 - Missing requirement on User Data padding
M4050007	SV8 - Key lifetime clarification
M6080004	SV8 - Directory Security Requirements

**EUROCONTROL Specification on the Air Traffic Services Message Handling System (AMHS)**

**Appendix 1**

**Traceability Matrix between SES Essential Requirements and EUROCONTROL Specification**

**TABLE OF CONTENTS**

Appendix 1. Traceability Matrix between SES Essential Requirements and EUROCONTROL Specification .....	2
A1.1 INTRODUCTION .....	2
A1.2 Essential Requirements mapping to EUROCONTROL Specification .....	2
A1.2.1 Essential Requirements – Part A .....	3
A1.2.2 Essential Requirements – Part B .....	8
A1.3 EUROCONTROL Specification mapping to Essential Requirements .....	11
A1.3.1 Annex A – Basic Service .....	12
A1.3.2 Annex B – Extended Service .....	22
A1.3.3 Annex C – Directory Service .....	27
A1.3.4 Annex D – Security .....	31

## APPENDIX 1. TRACEABILITY MATRIX BETWEEN SES ESSENTIAL REQUIREMENTS AND EUROCONTROL SPECIFICATION

### A1.1 INTRODUCTION

This informational Appendix provides traceability between the Essential Requirements (ER) in Annex II of the SES Interoperability Regulation [1] and the tagged requirements in the Annexes of the EUROCONTROL Specification on the Air Traffic Services Message Handling System (AMHS).

### A1.2 Essential Requirements mapping to EUROCONTROL Specification

*Note 1: The following table lists the ERs as given in Annex II of the Interoperability Regulation 552/2004 [1], and assigns reference numbers to individual paragraphs. The complete set of ERs is shown for completeness; ERs that are not considered relevant for ATS messaging systems are shown shaded.*

*The ERs are divided into parts A (General requirements) and B (Specific requirements per system type) each containing numbered sections with one requirement per paragraph; since there are multiple unnumbered paragraphs (and hence requirements) in some sections and subsections, individual requirements are identified by adding a paragraph number to the section number using the following format:*

*ER Reference: Part-Section-Paragraph*

*Where Part and Section correspond to the numbering in Annex II of the Interoperability Regulation and Paragraph denotes the paragraph number preceded by a P.*

*For example the tag: **B-3.1.2-P3** - denotes Annex II Part B, section 3.1.2, paragraph 3.*

*Note 2: Every requirement and recommendation in the EUROCONTROL Specification is identified by a structured tag, which can be used to reference uniquely the requirement / recommendation. The structure of requirement identifiers allows differentiation between the Basic ATSMHS and Extended ATSMHS and also identifies the major system components, which can be considered as candidate EATMN constituents. Such identifiers have the form:*

*AMHS-[Fn]-[Ann]*

*where:*

*[Fn]: is a sequence of characters to identify the operational procedure or category to which the requirement applies, e.g. “AMU” for requirements specific to ATS Message User Agent, “AMS” for requirements specific to ATS Message Server, “DIR” for general requirements related to Directory functions.*

*[Ann]: is the Annex identifier followed by a number, unique within a given [Fn], taking the value “A” for requirements specific to the Basic ATSMHS, “B” for requirements specific to the Extended ATSMHS, “C” for requirements specific to Directory functions and “D” for requirements specific to Security functions.*

**A1.2.1 Essential Requirements – Part A**

**Table 1: Essential Requirements - Part A**

ER Reference	Requirement Description	EUROCONTROL Specification Reference
<b>Part A: GENERAL REQUIREMENTS</b>		
<b>1. Seamless operation</b>		
A-1-P1	Air traffic management systems and their constituents shall be designed, built, maintained and operated using the appropriate and validated procedures, in such a way as to ensure the seamless operation of the EATMN at all times and for all phases of flight. Seamless operation can be expressed, in particular, in terms of information sharing, including the relevant operational status information, common understanding of information, comparable processing performances and the associated procedures enabling common operational performances agreed for the whole or parts of the EATMN.	<p>[AMHS-BAS-A01], [AMHS-BAS-A03], [AMHS-BAS-A04], [AMHS-BAS-A05], [AMHS-BAS-A06], [AMHS-BAS-A07], [AMHS-MGT-A26], [AMHS-CA-A01], [AMHS-CA-A02], [AMHS-CA-A03], [AMHS-CA-A04], [AMHS-CA-A05], [AMHS-CA-A06]</p> <p>[AMHS-BAS-B01], [AMHS-BAS-B03], [AMHS-CA-B01], [AMHS-CA-B02], [AMHS-CA-B03], [AMHS-CA-B04], [AMHS-CA-B05], [AMHS-CA-B06]</p> <p>[AMHS-DIR-C04]</p> <p>Note: Contributions are made to this requirement by specifying:</p> <ul style="list-style-type: none"> <li>a) A coherent ATS Message Handling Service and operational concepts throughout the applicable area.</li> <li>b) A communications system supporting a seamless relationship between ground-based systems, so that a service is not disrupted by breaks in coverage or wide variations in quality of service.</li> </ul>

ER Reference	Requirement Description	EUROCONTROL Specification Reference
<b>2. Support for new concepts of operation</b>		
A-2-P1	<p>The EATMN, its systems and their constituents shall support, on a coordinated basis, new agreed and validated concepts of operation that improve the quality and effectiveness of air navigation services, in particular in terms of safety and capacity.</p> <p><i>Note SES-II proposed amendment:</i></p> <p><i>'The EATMN, its systems and their constituents shall support, on a coordinated basis, new agreed and validated concepts of operation that improve the quality, sustainability and effectiveness of air navigation services, in particular in terms of safety and capacity.'</i></p>	<p>[AMHS-ARM-A01] [AMHS-GEN-B01], [AMHS-GEN-B02], [AMHS-GEN-B03] [AMHS-DIR-C01], [AMHS-DIR-C02], [AMHS-DIR-C09], [AMHS-DIR-C12], [AMHS-DIR-C13], [AMHS-DIR-C14], [AMHS-DIR-C33], [AMHS-DIR-C34], [AMHS-DIR-C35]</p> <p><i>Note:</i></p> <p><i>This requirement influences the specification in terms of the co-ordinated introduction of:</i></p> <ul style="list-style-type: none"> <li>a) <i>New concept of operations based on high capacity, secure, reliable digital communications;</i></li> <li>b) <i>Validated technology(ies) supporting data communications in the timeframe to 2020.</i></li> </ul>
A-2-P2	<p>The potential of new concepts, such as collaborative decision-making, increasing automation and alternative methods of delegation of separation responsibility, shall be examined taking due account of technological developments and of their safe implementation, following validation.</p>	<p>[AMHS-BAS-B02], [AMHS-GEN-B01], [AMHS-GEN-B02], [AMHS-GEN-B03], [AMHS-AMS-B01], [AMHS-AMS-B02], [AMHS-AMS-B03], [AMHS-AMS-B04], [AMHS-AMS-B05], [AMHS-AMS-B06], [AMHS-AMU-B02], [AMHS-AMU-B04], [AMHS-AMU-B06], [AMHS-AMU-B07], [AMHS-AMU-B08], [AMHS-AMU-B09], [AMHS-AMU-B10], [AMHS-AMU-B11], [AMHS-AMU-B12], [AMHS-AMU-B13], [AMHS-AMU-B14], [AMHS-AMU-B15], [AMHS-MST-B01], [AMHS-MST-B02], [AMHS-MST-B03], [AMHS-MST-B04], [AMHS-MST-B05], [AMHS-MST-B06], [AMHS-MST-B07], [AMHS-MST-B08], [AMHS-MST-B09], [AMHS-GWY-B01], [AMHS-GWY-B02] [AMHS-DIR-C01], [AMHS-DIR-C02]</p>
<b>3. Safety</b>		
A-3-P1	<p>Systems and operations of the EATMN shall achieve agreed high levels of safety. Agreed safety management and reporting methodologies shall be established to achieve this.</p>	<p>[AMHS-SAF-A01], [AMHS-SAF-A02], [AMHS-SAF-A05] [AMHS-SEC-D02]</p> <p><i>Note:</i></p> <p><i>Contributions are made to this requirement by specifying basic safety requirements applicable to systems and constituents implementing the ATSMHS.</i></p>

ER Reference	Requirement Description	EUROCONTROL Specification Reference
A-3-P2	In respect of appropriate ground-based systems, or parts thereof, these high levels of safety shall be enhanced by safety nets which shall be subject to agreed common performance characteristics.	Note: This is assumed to apply only to ATM systems, with safety nets such as MSAW, STCA, etc.
A-3-P3	A harmonised set of safety requirements for the design, implementation, maintenance and operation of systems and their constituents, both for normal and degraded modes of operation, shall be defined with a view to achieving the agreed safety levels, for all phases of flight and for the entire EATMN.	<p>[AMHS-SAF-A03], [AMHS-SAF-A04] [AMHS-SEC-D01]</p> <p><i>Note:</i> <i>Contributions are made to this requirement by specifying data communications mechanisms providing alternative communication paths between users.</i></p>
A-3-P4	Systems shall be designed, built, maintained and operated, using the appropriate and validated procedures, in such a way that the tasks assigned to the control staff are compatible with human capabilities, in both the normal and degraded modes of operation, and are consistent with required safety levels.	Note: This is assumed to apply only to ATC systems, where the “control staff” are ATCOs.

ER Reference	Requirement Description	EUROCONTROL Specification Reference
A-3-P5	Systems shall be designed, built, maintained and operated using the appropriate and validated procedures, in such a way as to be free from harmful interference in their normal operational environment.	<p>[AMHS-SAF-A06], [AMHS-MGT-A20], [AMHS-MGT-A21], [AMHS-MGT-A22], [AMHS-MGT-A23]  [AMHS-DIR-C07], [AMHS-DIR-C08], [AMHS-DIR-C14], [AMHS-DIR-C34]  [AMHS-SEC-D01], [AMHS-SEC-D04], [AMHS-SEC-D05], [AMHS-SEC-D06], [AMHS-SEC-D07], [AMHS-SEC-D08], [AMHS-SEC-D09], [AMHS-SEC-D10], [AMHS-SEC-D11], [AMHS-SEC-D12], [AMHS-SEC-D13], [AMHS-SEC-D14], [AMHS-SEC-D15], [AMHS-SEC-D16], [AMHS-SEC-D17], [AMHS-SEC-D18], [AMHS-SEC-D19], [AMHS-SEC-D20], [AMHS-SEC-D21], [AMHS-SEC-D22], [AMHS-SEC-D23], [AMHS-SEC-D24], [AMHS-SEC-D25], [AMHS-SEC-D26], [AMHS-SEC-D27], [AMHS-SEC-D28], [AMHS-SEC-D29], [AMHS-SEC-D30], [AMHS-SEC-D31], [AMHS-SEC-D32], [AMHS-SEC-D33], [AMHS-SEC-D34], [AMHS-SEC-D35], [AMHS-SEC-D36], [AMHS-SEC-D37], [AMHS-SEC-D38], [AMHS-SEC-D39], [AMHS-SEC-D40], [AMHS-SEC-D41], [AMHS-SEC-D42], [AMHS-SEC-D43], [AMHS-SEC-D44], [AMHS-SEC-D45], [AMHS-SEC-D46], [AMHS-SEC-D47], [AMHS-SEC-D48], [AMHS-SEC-D49], [AMHS-SEC-D50], [AMHS-SEC-D51], [AMHS-SEC-D52], [AMHS-SEC-D54]</p> <p><i>Note:</i>  Contributes to this requirement within the Extended ATSMHS; security services help to protect against safety hazards such as accidental or deliberate message corruption and provide protection against undetected misdelivery. Directory services also help to provide misdelivery protection.</p>
<b>4. Civil-military coordination</b>		
A-4-P1	The EATMN, its systems and their constituents shall support the progressive implementation of civil/military coordination, to the extent necessary for effective airspace and air traffic flow management, and the safe and efficient use of airspace by all users, through the application of the concept of the flexible use of airspace.	Main Body section 2.11
A-4-P2	To achieve these objectives, the EATMN, its systems and their constituents shall support the timely sharing of correct and consistent information covering all phases of flight, between civil and military parties.	[AMHS-AMS-A12]
A-4-P3	Account should be taken of national security requirements.	

ER Reference	Requirement Description	EUROCONTROL Specification Reference
<b>5. Environmental constraints</b>		
A-5-P1	Systems and operations of the EATMN shall take into account the need to minimise environmental impact in accordance with Community legislation.	<p><i>Note:</i></p> <p><i>Indirectly, improved data communication services enable concepts leading to reduced paper-based transactions and the need to travel to meetings, etc. However, this EUROCONTROL Specification does not contribute directly to ER5.</i></p>
<b>6. Principles governing the logical architecture of systems</b>		
A-6-P1	Systems shall be designed and progressively integrated with the objective of achieving a coherent and increasingly harmonised, evolutionary and validated logical architecture within the EATMN.	<p>[AMHS-ARM-A09]</p> <p><i>Note:</i></p> <p><i>Standardised data communication services support a common view of the logical architecture, at least at the level of the communications subsystems and of the communicating application processes. This EUROCONTROL Specification is based on ICAO provisions, which specify the X.400 architecture of MTAs, UAs, Message Stores and Access Units. Beyond this, the Specification does not prescribe any particular solution for the logical architecture of systems.</i></p>
<b>7. Principles governing the construction of systems</b>		



ER Reference	Requirement Description	EUROCONTROL Specification Reference
A-7-P1	Systems shall be designed, built and maintained on the grounds of sound engineering principles, in particular those relating to modularity, enabling interchangeability of constituents, high availability, and redundancy and fault tolerance of critical constituents.	<p>[AMHS-GEN-A04], [AMHS-GEN-A05], [AMHS-GEN-A08], [AMHS-SAF-A07], [AMHS-PER-A07], [AMHS-PER-A09], [AMHS-LOG-A01], [AMHS-LOG-A02], [AMHS-LOG-A03], [AMHS-LOG-A04], [AMHS-ARM-A02], [AMHS-ARM-A03], [AMHS-ARM-A10], [AMHS-MGT-A01], [AMHS-MGT-A05], [AMHS-MGT-A06], [AMHS-MGT-A07], [AMHS-MGT-A08], [AMHS-MGT-A09], [AMHS-MGT-A10], [AMHS-MGT-A11], [AMHS-MGT-A12], [AMHS-MGT-A13], [AMHS-MGT-A14], [AMHS-MGT-A16], [AMHS-MGT-A17], [AMHS-MGT-A18], [AMHS-MGT-A19], [AMHS-MGT-A24], [AMHS-MGT-A25], [AMHS-AMS-A07], [AMHS-AMS-A08], [AMHS-AMS-A09]</p> <p><i>Note:</i> Standardised data communication elements are designed to be modular, and are decoupled from specific exchange mechanisms and communications subnetworks. In the Extended ATSMHS, access protocols between UA and MTA are standardised, opening up the possibility to source UAs from different suppliers. However, this EUROCONTROL Specification does not prescribe the construction of systems in terms of modularity, high availability, redundancy and fault tolerance of critical constituents</p>

### A1.2.2 Essential Requirements – Part B

Table 2: Essential Requirements - Part B

ER Reference	Requirement Description	EUROCONTROL Specification Reference
<b>Part B: SPECIFIC REQUIREMENTS</b>		
<b>3.</b>	<b><i>Systems and procedures for air traffic services</i></b>	
<b>3.1</b>	<b>Flight data processing systems</b>	
3.1.1	Seamless operation	

ER Reference	Requirement Description	EUROCONTROL Specification Reference
B-3.1.1-P1	Flight data processing systems shall be interoperable in terms of the timely sharing of correct and consistent information, and a common operational understanding of that information, in order to ensure a coherent and consistent planning process and resource-efficient tactical coordination throughout the EATMN during all phases of flight.	
B-3.1.1-P2	In order to ensure safe, smooth and expeditious processing throughout the EATMN, flight data processing performances shall be equivalent and appropriate for a given environment (surface, terminal manoeuvring area (TMA), en-route), with known traffic characteristics and exploited under an agreed and validated operational concept, in particular in terms of accuracy and error tolerance of processing results.	
3.1.2 Support for new concepts of operation		
B-3-1.2-P1	Flight data processing systems shall accommodate the progressive implementation of advanced, agreed and validated concepts of operation for all phases of flight. <i>Note SES-II proposed amendment:</i> <i>'Flight data processing systems shall accommodate the progressive implementation of advanced, agreed and validated concepts of operation for all phases of flight, in particular as envisaged in the ATM Master Plan.'</i>	
B-3-1.2-P2	The characteristics of automation-intensive tools must be such as to enable coherent and efficient pre-tactical and tactical processing of flight information in parts of the EATMN.	
B-3-1.2-P3	Airborne and ground systems and their constituents supporting new, agreed and validated concepts of operation shall be designed, built, maintained and operated, using appropriate and validated procedures, in such a way as to be interoperable in terms of timely sharing of correct and consistent information and a common understanding of the current and predicted operational situation.	[AMHS-PER-A07] <i>Note: Flight Data Processing Systems are relevant, insofar as they may interface to the AMHS as direct "host" users.</i>
<b>4. Communication systems and procedures for ground-to-ground, air-to-ground and air-air communication</b>		
<b>4.1 Seamless operation</b>		
B-4.1-P1	Communication systems shall be designed, built, maintained and operated using the appropriate and validated procedures, in such a way as to achieve the required performances within a given volume of airspace or for a specific application, in particular in terms of communication processing time, integrity, availability and continuity of function.	[AMHS-GEN-A01], [AMHS-GEN-A02], [AMHS-GEN-A03], [AMHS-GEN-A04], [AMHS-GEN-A05], [AMHS-GEN-A06], [AMHS-GEN-A07], [AMHS-GEN-A08], [AMHS-PER-A01], [AMHS-PER-A02], [AMHS-PER-A04], [AMHS-PER-A05], [AMHS-PER-A06], [AMHS-PER-A07], [AMHS-PER-A08], [AMHS-ARM-A04], [AMHS-ARM-A05], [AMHS-ARM-A06], [AMHS-ARM-A07], [AMHS-ARM-A08], [AMHS-MGT-A02],

ER Reference	Requirement Description	EUROCONTROL Specification Reference
		<p>[AMHS-MGT-A03], [AMHS-MGT-A04], [AMHS-AMS-A01], [AMHS-AMS-A02], [AMHS-AMS-A03], [AMHS-AMS-A04], [AMHS-AMS-A05], [AMHS-AMS-A06], [AMHS-AMS-A07], [AMHS-AMS-A08], [AMHS-AMS-A09], [AMHS-AMS-A10], [AMHS-AMS-A11], [AMHS-AMU-A01], [AMHS-AMU-A02], [AMHS-AMU-A03], [AMHS-AMU-A04], [AMHS-AMU-A05], [AMHS-AMU-A06], [AMHS-AMU-A07], [AMHS-MST-A01], [AMHS-MST-A02], [AMHS-MST-A03], [AMHS-MST-A04], [AMHS-MST-A05], [AMHS-GWY-A01], [AMHS-GWY-A02], [AMHS-GWY-A03], [AMHS-GWY-A04], [AMHS-GWY-A05], [AMHS-GWY-A06], [AMHS-GWY-A07]</p>
B-4.1-P2	The communications network within the EATMN shall be such as to meet the requirements of quality of service, coverage and redundancy.	[AMHS-PER-A03]
<b>4.2 Support for new concepts of operation</b>		
B-4.2-P1	<p>Communication systems shall support the implementation of advanced, agreed and validated concepts of operation for all phases of flight.</p> <p><i>Note SES-II proposed amendment:</i></p> <p><i>'Communication systems shall support the implementation of advanced, agreed and validated concepts of operation for all phases of flight, in particular as envisaged in the ATM Master Plan.'</i></p>	<p>[AMHS-N&amp;A-B01], [AMHS-AMU-B01], [AMHS-AMU-B03], [AMHS-AMU-B04]</p> <p>[AMHS-DIR-C03], [AMHS-DIR-C05], [AMHS-DIR-C06], [AMHS-DIR-C07], [AMHS-DIR-C08], [AMHS-DIR-C10], [AMHS-DIR-C11], [AMHS-DIR-C15], [AMHS-DIR-C16], [AMHS-DIR-C17], [AMHS-DIR-C18], [AMHS-DIR-C19], [AMHS-DIR-C29], [AMHS-DIR-C22], [AMHS-DIR-C23], [AMHS-DIR-C24], [AMHS-DIR-C25], [AMHS-DIR-C26], [AMHS-DIR-C27], [AMHS-DIR-C28], [AMHS-DIR-C29], [AMHS-DIR-C30], [AMHS-DIR-C31], [AMHS-DIR-C32], [AMHS-CA-C01], [AMHS-CA-C02], [AMHS-CA-C03], [AMHS-CA-C04], [AMHS-CA-C05], [AMHS-CA-C06], [AMHS-CA-C07]</p>

### A1.3 EUROCONTROL Specification mapping to Essential Requirements

The tables in this section map the tagged requirements to paragraphs in the ER (see note in section A1.2). In addition the tables contain a classification of how each requirement can be tested for conformance during validation and testing.

*Note: It is assumed that one or more test specifications will be produced for testing conformance to the EUROCONTROL Specification (“the Specification”), in this document “Test Specification” is the term used.*

The testing categories are as follows:

<b>Test</b>	<u>The Requirement may be tested and a definite result obtained</u>  An assessment where the conformity of an implementation to the Specification Requirement is measured at a quantitative level, through the application of defined input stimuli and comparison of the resulting outputs with what is specified in the Test Specification.
<b>Demonstrate</b>	<u>The testing of the Specification Requirement cannot be defined by this document, but must be demonstrated by the implementer to meet the requirement.</u>  An assessment where the conformity of the implementation to the Specification Requirement can only be assessed at a qualitative level, through the execution of a defined procedure which shows how the implementation meets the requirement of the Specification.
<b>Evaluate</b>	<u>The Requirement may be tested or demonstrated and a full, or partial, result obtained</u>  An assessment where the conformity of the implementation to the Specification Requirement can only be assessed by a test or demonstration, the results of which only meet the notional requirement in part. The results are evaluated by the test scrutinisers to assess the degree to which the requirement has been met.
<b>Audit</b>	<u>The Requirement cannot be tested, but must be assessed by other means</u>  The conformity of the implementation must be assessed by means other than testing or demonstration, e.g. inspection of the documentation, design processes, inspection records, design review records.

A1.3.1 Annex A – Basic Service

Table 3: Annex A – Basic Service

Requirement Reference	Requirement Description	Essential Requirements Reference	Test	Demo	Eval	Audit	Notes
<b>A.2 REQUIREMENTS AND EXPLANATORY MATERIALS</b>							
<b>A.2.1 Common Requirements</b>							
<i>A.2.1.1 Standards Baseline</i>							
[AMHS-BAS-A01]	AMHS End Systems shall comply with the requirements identified in ICAO EUR Doc 020 [8] unless otherwise explicitly stated in this EUROCONTROL Specification.	A-1-P1, A-2-P1				X	
[AMHS-BAS-A03]	AMHS End Systems shall comply with the requirements specified in ICAO Doc 9880 Part IIB [5] applicable to the Basic ATSMHS, except where explicitly stated otherwise.	A-1-P1, A-2-P1				X	
[AMHS-BAS-A04]	In the event of conflicting requirements not explicitly identified, the specification in ICAO Doc 9880 Part IIB [5] shall take precedence.	A-1-P1, A-2-P1				X	
[AMHS-BAS-A05]	Due account shall be taken of any published defect resolutions relating to the ICAO AMHS documentation.	A-1-P1, A-2-P1				X	
[AMHS-BAS-A06]	Implementations of AMHS Components shall conform to the 2003 version of the MHS base standards [18] and the 2003 version of the referenced International Standardized Profiles (ISPs) [19], [20].	A-1-P1, A-2-P1				X	PICS will be supplied
[AMHS-BAS-A07]	Compatibility with the current version of referenced standards and any relevant corrigenda should be taken into account.	A-1-P1, A-2-P1				X	
<i>A.2.1.2 General Requirements</i>							
[AMHS-GEN-A01]	The AMHS shall enable the exchange of messages between the following types of users: <ul style="list-style-type: none"> <li>• direct AMHS user to direct AMHS user;</li> <li>• direct AMHS user to indirect AMHS user and vice-versa;</li> <li>• indirect AMHS user to direct AMHS user;</li> <li>• indirect AMHS user to indirect AMHS user.</li> </ul>	B-4.1-P1	X				
[AMHS-GEN-A02]	AMHS Components shall be able to communicate using the TCP/IP Transport Service, as specified in ICAO Doc 9880 Part IIB [5] section 3.2.2.2.3.	B-4.1-P1		X			
[AMHS-GEN-A03]	AMHS End System implementations should follow the “Guidelines for system requirements” in section 5 of ICAO EUR Doc 020 [8].	B-4.1-P1				X	
[AMHS-GEN-A04]	Wherever possible, AMHS Component implementations should make use of common and standardised interfaces.	B-4.1-P1, A-7-P1				X	
[AMHS-GEN-A05]	Specifically, standardised interfaces where available for message submission, transfer and delivery, system management, etc. shall be used as a means of enhancing Interoperability between system components.	B-4.1-P1, A-7-P1				X	

Requirement Reference	Requirement Description	Essential Requirements Reference	Test	Demo	Eval	Audit	Notes
[AMHS-GEN-A06]	AMHS End Systems should support by local means the object classes and attribute types of directory information specified in ICAO EUR Doc 020 [8] Appendix B Annex K, with a (local) mechanism to obtain such information by a UA, MTA or MTCU component.	B-4.1-P1				X	
[AMHS-GEN-A07]	AMHS End Systems shall be capable of interworking with independent implementations of AMHS End Systems in accordance with the permissible combinations listed in ICAO Doc 9880 Part IIB [5] section 1.2.	B-4.1-P1	X				
[AMHS-GEN-A08]	AMHS End Systems supporting the Basic ATSMHS shall be designed to accommodate the evolution to support the Extended ATSMHS, e.g. by including well-defined interfaces and software hooks in areas where future extensions are foreseen.	B-4.1-P2, A-7-P1				X	
<i>A.2.1.3 Safety Requirements</i>							
[AMHS-SAF-A01]	As for any EATMN system or constituent, a safety assessment shall be performed for the initial planned use of the ATSMHS.	A-3-P1				X	
[AMHS-SAF-A02]	Procedures shall be put in place to ensure that a further safety assessment is performed as and when additional end-user applications making use of the ATSMHS are deployed.	A-3-P1				X	
[AMHS-SAF-A03]	AMHS End Systems and operations in the EATMN shall achieve agreed high levels of safety using established safety management and reporting methodologies.	A-3-P3				X	
[AMHS-SAF-A04]	A harmonised set of safety requirements for the design, implementation, maintenance and operation of AMHS End Systems, both for normal and degraded modes of operation, shall be applied with a view to achieving the agreed safety levels for the entire AMHS.	A-3-P3				X	
[AMHS-SAF-A05]	AMHS End Systems shall be designed, built, maintained and operated, using the appropriate and validated procedures, in such a way that the tasks assigned to the control staff are compatible with human capabilities, in both the normal and degraded modes of operation, and are consistent with required safety levels.	A-3-P4				X	
[AMHS-SAF-A06]	AMHS End Systems shall be designed, built, maintained and operated using the appropriate and validated procedures, in such a way as to be free from harmful interference in their normal operational environment.	A-3-P5				X	
<i>A.2.1.3.1 Software Assurance Level</i>							
[AMHS-SAF-A07]	The allocated software assurance level shall be commensurate with the most adverse effect that software malfunctions or failures may cause, taking into account the risks associated with software malfunctions or failures and the architectural and/or procedural defences identified.	A-7-P1				X	
<i>A.2.1.4 Performance Requirements</i>							

Requirement Reference	Requirement Description	Essential Requirements Reference	Test	Demo	Eval	Audit	Notes
[AMHS-PER-A01]	An operational performance assessment (OPA, as defined in EUROCAE Document ED-78A [11]) shall be performed for the initial planned use of the ATSMHS.	B-4.1-P1				X	
[AMHS-PER-A02]	Procedures shall be put in place to ensure that a further OPA is performed as and when additional end-user applications making use of the ATSMHS are deployed.	B-4.1-P1				X	
[AMHS-PER-A03]	The ATSMHS within the EATMN shall be such as to meet the requirements of quality of service, coverage and redundancy as required for the supported applications.	B-4.1-P2				X	
[AMHS-PER-A04]	When adding new services, the affect of the additional message traffic on the existing traffic shall be considered.	B-4.1-P1				X	
[AMHS-PER-A05]	AMHS End Systems shall be designed, built, maintained and operated using the appropriate and validated procedures, in such a way as to achieve the required performances for a specific application, in particular in terms of: a) communication processing time, b) integrity, c) availability and d) continuity of function.	B-4.1-P1			X		
[AMHS-PER-A06]	AMHS End Systems shall be designed and dimensioned to enable the end-to-end performance requirements for each “QoS Flow Type Class” listed in ICAO EUR Doc 020 [8], section 3.1.4, Table 1 to be met.	B-4.1-P1			X		
[AMHS-PER-A07]	AMHS End Systems and their constituents supporting new, agreed and validated concepts of operation shall be designed, built, maintained and operated, using appropriate and validated procedures, in such as way as to be interoperable in terms of timely sharing of correct and consistent information.	A-7-P1, B-3-1.2-P3, B-4.1-P1				X	
[AMHS-PER-A08]	AMHS End Systems should be capable of supporting the peak rate hour's performance, which corresponds to at least 20% of the daily traffic requirements for that AMHS End System.	B-4.1-P2			X		
[AMHS-PER-A09]	An AMHS End System shall comply, to the extent possible, with the sizing recommendations specified in section 5.7 of ICAO EUR Doc 020 [8].	A-7-P1				X	
<i>A.2.1.5 Naming and Addressing</i>							
<i>A.2.1.6 Logging</i>							
[AMHS-LOG-A01]	Data exchanges using the ATSMHS shall be recorded in accordance with the following ICAO standards applicable to the ground-based recording function of data link communications: • Section 3.5.1.5 of ICAO Annex 10 Volume II [3]; • Section 6.2 of ICAO Annex 11 [4]	A-7-P1		X			

Requirement Reference	Requirement Description	Essential Requirements Reference	Test	Demo	Eval	Audit	Notes
[AMHS-LOG-A02]	EUROCAE ED-111 [12] shall be considered as sufficient means of compliance of the ground-based recording function with regard to the identified ICAO standards applicable to the ground-based recording function of ATS data communications.	A-7-P1				X	
[AMHS-LOG-A03]	AMHS End Systems shall support the relevant requirements for traffic logging as described in sections 2.7, 3.2.3 and 4.3.1 of ICAO Doc 9880 Part IIB [5]	A-7-P1		X			
[AMHS-LOG-A04]	All operator inputs shall be recorded and traceable for a configurable period (e.g. 30 days).	A-7-P1	X				
<i>A.2.1.7 Availability, Reliability, Maintainability</i>							
[AMHS-ARM-A01]	A reliability, availability and maintainability analysis shall be conducted before entry into service and periodically thereafter to verify that AMHS End Systems satisfy or exceed the minimum requirements in these areas.	A-2-P1				X	
<i>A.2.1.7.1 Availability</i>							
[AMHS-ARM-A02]	An ATS Message Server and AFTN/AMHS Gateway shall be available 24 hours per day, with availability (defined as lack of unplanned outages) of at least 99.999% per year.	A-7-P1			X		
[AMHS-ARM-A03]	An ATS Message User Agent shall be available as required, with availability of at least 99.99% per year.	A-7-P1			X		
[AMHS-ARM-A04]	Precise constraints for the restart time are dependent on the configuration of the system and specific modes of failure, but for guidance a target restart time of less than 5 minutes shall be assumed.	B-4.1-P1			X		
[AMHS-ARM-A05]	Components and system modes of failure which imply a restart time of more than 1 minute shall be identified.	B-4.1-P1			X		
[AMHS-ARM-A06]	AMHS End Systems shall be designed such that processing of messages during recovery does not overload the system or degrade the performance below the performance targets.	B-4.1-P1				X	
<i>A.2.1.7.2 Reliability</i>							
[AMHS-ARM-A07]	AMHS End Systems shall be designed to minimise the effect of a failure of an AMHS End System or component thereof on the function of the entire system.	B-4.1-P1				X	
[AMHS-ARM-A08]	AMHS End Systems and their functional components shall be designed to avoid loss of messages.	B-4.1-P1				X	
<i>A.2.1.7.3 Maintainability</i>							
[AMHS-ARM-A09]	Commercial Off-the-Shelf (COTS), industry standard software, should be used as widely as possible, in order to enable an upward compatible growth path.	A-6-P1				X	



Requirement Reference	Requirement Description	Essential Requirements Reference	Test	Demo	Eval	Audit	Notes
[AMHS-ARM-A10]	AMHS End System implementations should be modular in nature and by using a series of industry standard interfaces provide a flexible and expandable combination of communication services.	A-7-P1				X	
<i>A.2.1.8 System Operation and Management</i>							
<i>A.2.1.8.1 Fault Management</i>							
[AMHS-MGT-A01]	AMHS End System implementations shall support fault management in all components.	A-7-P1				X	
[AMHS-MGT-A02]	It should be possible to schedule the execution of diagnostic tests.	B-4.1-P1		X			
[AMHS-MGT-A03]	On detection of a fault condition, depending upon the fault severity and classification, AMHS End Systems should be configurable to perform one or more of the following actions, in increasing order of severity: a) Reconfigure; b) Switch over or re-assign resources; c) Perform software re-initialisation; d) Perform hardware re-initialisation.	B-4.1-P1	X				
[AMHS-MGT-A04]	All fault conditions and actions shall be logged and remain accessible for a configurable period of not less than 1 month.	B-4.1-P1		X			
[AMHS-MGT-A05]	The maximum period for stored events shall not be limited by the system design, and only be constrained by management configuration or the available resources of the specific system.	A-7-P1			X		
[AMHS-MGT-A06]	An AMHS End System shall be able to meet its performance requirements when generation and storage of additional information (tracing) in support of basic failure analysis is enabled.	A-7-P1			X		
<i>A.2.1.8.2 Configuration Management</i>							
[AMHS-MGT-A07]	AMHS End Systems shall support the configuration management of all components.	A-7-P1		X			
[AMHS-MGT-A08]	Where applicable, the AMHS End System or specific component should allow the on-line modification and activation of configuration parameters without requiring an interruption of service.	A-7-P1		X			
[AMHS-MGT-A09]	The configuration, maintenance and activation of new addressing and routing information shall be possible through on-line modification without stopping the AMHS End System or substantially impairing its performance.	A-7-P1			X		
[AMHS-MGT-A10]	The design of an AMHS End System shall not constrain the size of the address space or addressing and routing tables; these are only constrained by system management configuration or available system resources.	A-7-P1				X	
[AMHS-MGT-A11]	All modifications of the application configuration should be logged.	A-7-P1		X			
[AMHS-MGT-A12]	AMHS End Systems should have the capability to import data specified in the address management function of the ATS Messaging Management Manual [9].	A-7-P1		X			

Requirement Reference	Requirement Description	Essential Requirements Reference	Test	Demo	Eval	Audit	Notes
A.2.1.8.3 Accounting Management							
A.2.1.8.4 Performance Management							
[AMHS-MGT-A13]	AMHS End System implementations shall support the collection and analysis of performance management data.	A-7-P1				X	
[AMHS-MGT-A14]	It should be possible for the collection of statistical data to be configured, including the use of filters and the specification of collection and consolidation intervals.	A-7-P1		X			
[AMHS-MGT-A16]	ATS Message Server implementations shall export statistics data in accordance with the format specified in the ATS Messaging Management Manual [9], Appendix C.	A-7-P1		X			
[AMHS-MGT-A17]	It should be possible to configure trigger conditions to automatically regulate and prevent processor or storage overloads.	A-7-P1		X			
[AMHS-MGT-A18]	Statistics shall be provided for overall performance, use of overall capacity, use of component capacity, overall availability and component availability.	A-7-P1		X			
[AMHS-MGT-A19]	Statistical data shall be stored and accessible for a configurable period of not less than 1 month.	A-7-P1		X			
A.2.1.8.5 Security Management							
[AMHS-MGT-A20]	AMHS End System implementations shall support security management functions, including management of access control lists, local user authentication and authorisation, in accordance with ICAO EUR AFS Security Guidelines [10]	A3-P5				X	
[AMHS-MGT-A21]	Access control mechanisms shall be provided to restrict access to system management information.	A3-P5		X			
[AMHS-MGT-A22]	User roles with configurable access rights should be supported.	A3-P5		X			
A.2.1.8.6 System Monitoring Functions							
[AMHS-MGT-A23]	All events, occurring due to automatically triggered changes to the AMHS End System configuration, components or subscribers as well as occurring due to forced changes shall be indicated on-line (e.g. as system messages).	A3-P5		X			
A.2.1.8.7 System Management Interface							
[AMHS-MGT-A24]	AMHS End System implementations shall include a systems management interface consistent with the provisions of ICAO EUR Doc 020 [8], with suitable access control.	A-7-P1				X	
[AMHS-MGT-A25]	Communication between the management interface and the system should be through the use of an SNMP [40] compatible interface, enabling interoperability between manager and agent components (see ICAO EUR Doc 020 [8], section 5.8.5).	A-7-P1				X	
A.2.1.9 Transitional Procedures							

Requirement Reference	Requirement Description	Essential Requirements Reference	Test	Demo	Eval	Audit	Notes
[AMHS-MGT-A26]	Procedures for the introduction of ATSMHS into an international COM Centre shall be as specified in Appendix A of ICAO EUR Doc 021, ATS Messaging Management Manual [9].	A-1-P1				X	
<b>A.2.2 ATS Message Server Requirements</b>							
[AMHS-AMS-A01]	An ATS Message Server shall route, store and forward ATS Messages, taking into account the applicable performance requirements and routing configuration.	B-4.1-P1		X			
[AMHS-AMS-A02]	An ATS Message Server shall be able to support the routing of messages according to a non-hierarchical addressing plan, as well as the MF-Addressing Schemes specified in ICAO Doc 9880 Part IIB [5] section 2.5.1.4.	B-4.1-P1		X			
[AMHS-AMS-A03]	An ATS Message Server should have the capability to import data specified in the routing management function of the ATS Messaging Management Manual [9]	B-4.1-P1		X			
[AMHS-AMS-A04]	MTAs shall implement the P1 MTS transfer profile as specified in Appendix B Annex F of ICAO EUR Doc 020 [8] (profile AMH11 plus AMHS-specific features), for communication with other ATS Message Servers.	B-4.1-P1				X	
[AMHS-AMS-A05]	MTAs shall implement the P1 IPM requirements profile as specified in Appendix B Annex B of ICAO EUR Doc 020 [8] (profile AMH22 plus AMHS-specific features), for IPM communication with other ATS Message Servers.	B-4.1-P1				X	
[AMHS-AMS-A06]	MTAs shall support a P1 message length of at least 2 MByte.	B-4.1-P1	X				
[AMHS-AMS-A07]	The ATS Message Server should support a common and standardised interface for the submission and delivery of messages.	A-7-P1, B-4.1-P1				X	
[AMHS-AMS-A08]	In support of the integration of an ATS Message User Agent into other computer applications, an API for the submission and delivery of messages using Open Group API specifications [38] may be specified.	B-4.1-P1				X	
[AMHS-AMS-A09]	MTAs shall support the Distribution List (DL) functional group.	B-4.1-P1	X				
[AMHS-AMS-A10]	It is recommended that the ATS Message Server should have the capability to open multiple associations between each pair of communicating MTAs (see ICAO EUR Doc 020 [8] section 5.2.2).	B-4.1-P1		X			
[AMHS-AMS-A11]	The ATS Message Server shall use the Monologue dialogue-mode of the RTSE protocol for associations between each pair of communicating MTAs.	B-4.1-P1			X		
<b>A.2.2.1 EATMN Boundary Requirements</b>							
[AMHS-AMS-A12]	EATMN boundary ATS Message Servers shall additionally have the capability to communicate with ATS Message Servers external to the EATMN, subject to bilateral agreement.	A-4-P2			X		
<b>A.2.3 ATS Message User Agent Requirements</b>							

Requirement Reference	Requirement Description	Essential Requirements Reference	Test	Demo	Eval	Audit	Notes
[AMHS-AMU-A01]	ATS Message User Agents shall comply with the requirements specified in section 3.1 of ICAO Doc 9880 Part IIB [5] for the support of the Basic ATSMHS, summarised as the following requirements: <ul style="list-style-type: none"> <li>• A UA profile based on AMH21 as specified in ISO/IEC ISP 12062-2 [20];</li> <li>• The requirements of Repertoire Group A, for messages including a body part whose type is an Extended Body Part Type of general-text-body-part type;</li> <li>• Provisions related to traffic logging</li> </ul>	B-4.1-P1				X	
[AMHS-AMU-A02]	It is recommended that standard ISO/IEC 10021 [18] protocols P3 and/or P7 should be used for message submission and delivery.	B-4.1-P1				X	
[AMHS-AMU-A03]	The maximum message-text length supported by the UA shall be a configurable parameter value.	B-4.1-P1	X				
[AMHS-AMU-A04]	A UA shall be capable of accepting and processing a maximum received message-text length of at least 64 kByte and be capable of handling messages longer than the maximum length without malfunction.	B-4.1-P1	X				
[AMHS-AMU-A05]	If a user application is co-located with an MTA on a common platform, then the interface between the application's (logical) UA and the message transfer service shall provide equivalent functionality to the MT-Access abstract service as defined for the P3 access protocol specified in ISO/IEC 10021-6 [18]	B-4.1-P1				X	
[AMHS-AMU-A06]	If "forced" delivery to a UA is required (e.g. for reception of urgent, high priority messages) then either the P3 protocol or (in the case of MS) P7 with Alerts configured should be used.	B-4.1-P1				X	
[AMHS-AMU-A07]	It should be possible for direct AMHS users to request confirmation of delivery and to receive delivery reports.	B-4.1-P1	X				
<b>A.2.4 Message Store Requirements</b>							
[AMHS-MST-A01]	It is recommended that, when an MS is included in the ATS Message Server, standard ISO/IEC 10021 [18] protocol P3 should be used between the MS and MTA for message submission and delivery.	B-4.1-P1				X	
[AMHS-MST-A02]	It is recommended that standard ISO/IEC 10021 [18] protocol P7 should be used between MS and UA for message retrieval and indirect submission.	B-4.1-P1				X	
[AMHS-MST-A03]	It is recommended that the MS application context should exclude the Reliable Transfer Service Element (RTSE).	B-4.1-P1				X	
[AMHS-MST-A04]	MS implementations may support the Distribution List (DL) functional group.	B-4.1-P1				X	
[AMHS-MST-A05]	Requirements for the maximum number of MS users that can be simultaneously supported by an MS implementation shall be based upon current and foreseen ATSMHS usage.	B-4.1-P1				X	

Requirement Reference	Requirement Description	Essential Requirements Reference	Test	Demo	Eval	Audit	Notes
<b>A.2.5 AFTN/AMHS Gateway Requirements</b>							
[AMHS-GWY-A01]	Where interworking with AFTN end systems is required, a gateway between the AMHS and AFTN message services shall be implemented in conformance with ICAO Doc 9880 Part IIB [5] chapter 4.	B-4.1-P1				X	
[AMHS-GWY-A02]	An AFTN/AMHS Gateway supporting the Basic ATSMHS shall implement all elements which are applicable to the Basic ATSMHS and which are marked as “M” in the “ATS Messaging Service” column of ICAO Doc 9880 Part IIB Table 4-3.	B-4.1-P1	X				
[AMHS-GWY-A03]	The AFTN/AMHS Gateway shall support address conversion of O/R addresses belonging to a non-hierarchical addressing plan, as well as the MF-Addressing Schemes specified in ICAO Doc 9880 Part IIB [5] section 2.5.1.4.	B-4.1-P1		X			
[AMHS-GWY-A04]	The AFTN/AMHS Gateway shall support address conversion and routing for all currently assigned ICAO eight-letter addressee indicators (AF-addresses).	B-4.1-P1		X			
[AMHS-GWY-A05]	The AFTN/AMHS Gateway should have the capability to import the address mapping tables in comma-separated value (CSV) format provided by the European ATS Messaging Management Centre (AMC).	B-4.1-P1		X			
[AMHS-GWY-A06]	If the length of the ATS-Message-Text element in an AMHS message exceeds the maximum supported length (a parameter set initially to 64 kByte, in accordance with current AFTN/CIDIN practices for the support of ADEXP messages), the message shall be rejected by the AFTN/AMHS Gateway's MTCU as specified in ICAO Doc 9880 Part IIB [5] section 4.5.2.1.7 a).	B-4.1-P1	X				
[AMHS-GWY-A07]	If the length of the ATS-Message-Text element in an AMHS message exceeds 1800 characters but does not exceed the maximum supported length, the AFTN component of the AFTN/AMHS Gateway shall handle the message using one of the following options, depending on the AFTN/CIDIN capability of the next international COM centres towards the destination: a) Transfer the message without modification; or b) Truncate the message text to 1800 characters; or c) Perform the message splitting procedure specified in ICAO Doc 9880 Part IIB [5] section 4.5.2.1.7 b).	B-4.1-P1	X				
<b>A.3 CONFORMITY ASSESSMENT MATERIALS</b>							
<b>A.3.1 Compliance Statement</b>							
[AMHS-CA-A01]	A claim of conformance for an implementation shall be supported by completion of the relevant Protocol Implementation Conformance Statement (PICS) pro forma.	A-1-P1, Annex IV-P4				X	Part of Technical File

Requirement Reference	Requirement Description	Essential Requirements Reference	Test	Demo	Eval	Audit	Notes
[AMHS-CA-A02]	Implementers claiming conformance to the specified services shall complete the PICS specified in Appendix B Annex Q of ICAO EUR Doc 020 [8].	A-1-P1, Annex IV-P4				X	Part of Technical File
[AMHS-CA-A03]	Implementers shall state whether all of the requirements and which of the optional elements of the AFTN/AMHS Gateway supporting the Basic ATSMHS as specified in ICAO Doc 9880 Part IIB [5] section 4 have been implemented, using the pro forma tables in this section, or equivalent.	A-1-P1, Annex IV-P4				X	Part of Technical File
[AMHS-CA-A04]	For AFTN/AMHS Gateway implementations, a PICS shall be provided stating the level of support, for each of the elements relevant to support of the Basic ATSMHS, listed in the profile requirements lists in section 4 of ICAO Doc 9880 Part IIB [5] and specified in Table A-2.	A-1-P1, Annex IV-P4				X	Part of Technical File
[AMHS-CA-A05]	AMHS End Systems shall be tested according to suitable test cases and procedures ensuring adequate coverage of the BASIC functional group.	A-1-P1, Annex IV-P4				X	Part of Technical File
[AMHS-CA-A06]	Testing shall be conducted within a common framework consistent with the procedures in ICAO EUR Doc 020 [8] using appropriate test tools and procedures.	A-1-P1, Annex IV-P4				X	Part of Technical File

**A1.3.2 Annex B – Extended Service**

**Table 4: Annex B – Extended Service**

Requirement Reference	Requirement Description	Essential Requirements Reference	Test	Demo	Eval	Audit	Notes
<b>B.2 REQUIREMENTS AND EXPLANATORY MATERIALS</b>							
<b>B.2.1 Common Requirements</b>							
<i>B.2.1.1 Standards Baseline</i>							
[AMHS-BAS-B01]	AMHS End Systems shall comply with the standards identified in Annex A of this EUROCONTROL Specification unless stated otherwise.	A-1-P1				X	
[AMHS-BAS-B02]	AMHS End Systems conforming to this Annex shall comply with the requirements specified in ICAO Doc 9880 Part IIB [5], including those requirements specific to the support of the Extended ATSMHS, unless explicitly stated otherwise in this Annex.	A-2-P2				X	
[AMHS-BAS-B03]	In the event of conflicting requirements not explicitly identified, the specification in ICAO Doc 9880 Part IIB [5] shall take precedence.	A-1-P1				X	
<i>B.2.1.2 General Requirements</i>							
[AMHS-GEN-B01]	ATS Message Servers and ATS Message User Agents shall conform to configuration IX as defined in ICAO Doc 9880 Part IIB [5] section 3.4 (i.e. functional groups Basic + IHE + DIR + FTBP), with the goal of future migration to configuration X (addition of functional group SEC).	A-2-P1, A-2-P2				X	
[AMHS-GEN-B02]	AMHS End Systems shall support the object classes and attribute types of directory information specified in ICAO EUR Doc 020 [8] Appendix B Annex K.	A-2-P1, A-2-P2				X	
[AMHS-GEN-B03]	AMHS End Systems shall support the implementation of advanced, agreed and validated concepts of operation by providing managed access to the messaging system for new end-user applications via well-defined interfaces.	A-2-P1, A-2-P2				X	
<i>B.2.1.3 Naming and Addressing</i>							
[AMHS-N&A-B01]	The responsible operators of AMHS Management Domains shall register a unique directory name for each AMHS user in their domain.	B-4.2-P1			X		
<i>B.2.1.4 Safety Requirements</i>							
<i>B.2.1.5 Performance Requirements</i>							
<b>B.2.2 ATS Message Server Requirements</b>							
<i>B.2.2.1 General</i>							
<i>B.2.2.2 P1 Message Transfer</i>							

Requirement Reference	Requirement Description	Essential Requirements Reference	Test	Demo	Eval	Audit	Notes
[AMHS-AMS-B01]	MTAs shall implement the P1 MTS transfer profile AMH11 as specified in Annex A of this EUROCONTROL Specification, with the addition of support of the DIR Functional Group as specified in ICAO Doc 9880 Part IIB [5] section 3.2.4.2.	A-2-P2				X	
[AMHS-AMS-B02]	MTAs should implement the SEC Functional Group of the P1 IPM requirements profile AMH22, for security class S0, in addition to the AMH22 requirements specified in Annex A of this EUROCONTROL Specification.	A-2-P2				X	
<b>B.2.2.3 P3 Message Transfer</b>							
[AMHS-AMS-B03]	MTAs supporting direct message submission and delivery shall support P3 access conforming to the profile in Appendix B Annex G of ICAO EUR Doc 020 [8].	A-2-P2				X	
[AMHS-AMS-B04]	MTAs supporting direct message submission and delivery shall support IPM P3 access conforming to the profile in Appendix B Annex C of ICAO EUR Doc 020 [8], with the addition of support of the DIR Functional Group as specified in ICAO Doc 9880 Part IIB [5] section 3.1.4.3.1.	A-2-P2				X	
[AMHS-AMS-B05]	MTAs should additionally implement the SEC Functional Group of the IPM P3 Access profile AMH23/AMH25, for security class S0.	A-2-P2				X	
<b>B.2.2.4 Directory Access</b>							
[AMHS-AMS-B06]	An ATS Message Server implementing the DIR functional group shall include a DUA for access to the ATN Directory.	A-2-P2				X	
<b>B.2.3 ATS Message Server Requirements</b>							
<b>B.2.3.1 General</b>							



Requirement Reference	Requirement Description	Essential Requirements Reference	Test	Demo	Eval	Audit	Notes
[AMHS-AMU-B01]	An ATS Message User Agent supporting the Extended ATSMHS shall comply with the requirements specified in section 3.1 of ICAO Doc 9880 Part IIB [5] for the support of the Extended ATSMHS, summarised as the following requirements; <ul style="list-style-type: none"> <li>• A UA profile based on Profile AMH21 as specified in ISO/IEC ISP 12062-2 [20];</li> <li>• The requirements of Repertoire Group A, for messages including a body part whose type is an Extended Body Part Type of general-text-body-part type;</li> <li>• Support of the IPM Business Class (BC) functional group as specified in ISO/IEC ISP 12062-2 [20]</li> <li>• Support of the file-transfer body part;</li> <li>• UA access profile based on Profiles AMH23 or AMH25 for P3 access to the MTS, or based on Profiles AMH24 or AMH26 for P7 access to the MS, as specified in ISO/IEC ISP 12062 [20] parts 4, 5 and 6;</li> <li>• The additional provisions relating to parameters generated at an ATS Message User Agent, as specified for the Extended ATSMHS;</li> <li>• Provisions related to traffic logging.</li> <li>• A DUA profile supporting the defined access profile and the specified object classes and attribute types.</li> </ul>	B-4.2-P1			X		
<b>B.2.3.2 IPM Content</b>							
[AMHS-AMU-B02]	A UA in an ATS Message User Agent supporting the Extended ATSMHS shall conform to the profile in Appendix B Annex A of ICAO EUR Doc 020 [8].	A-2-P2				X	
[AMHS-AMU-B03]	A UA in an ATS Message User Agent shall be prohibited from sending messages containing a Bilaterally Defined body part.	B-4.2-P1		X			
[AMHS-AMU-B04]	A UA shall additionally implement the elements of the BC Functional Group of the IPM Content profile AMH21 indicated as “m” in the “Support” column of Table B-1, as specified in ICAO Doc 9880 Part IIB [5], section 3.1.4.2.1.	B-4.2-P1	X				
[AMHS-AMU-B05]	The values of the <i>precedence</i> field in the per-recipient heading fields of a message shall be the same for all recipients, as this field corresponds to AFTN Priority.	A-2-P2	X				
<b>B.2.3.3 P3 Access</b>							
[AMHS-AMU-B06]	A UA supporting P3 access shall conform to the profile in Appendix B Annex G of ICAO EUR Doc 020 [8].	A-2-P2				X	
[AMHS-AMU-B07]	A UA supporting P3 access shall conform to the profile in Appendix B Annex C of ICAO EUR Doc 020 [8], with the addition of support of the DIR Functional Group as specified in ICAO Doc 9880 Part IIB [5] section 3.1.4.3.1.	A-2-P2				X	

Requirement Reference	Requirement Description	Essential Requirements Reference	Test	Demo	Eval	Audit	Notes
[AMHS-AMU-B08]	It is recommended that a UA supporting P3 access should conform to the MTS Access profile AMH23.	A-2-P2				X	
[AMHS-AMU-B09]	A UA should additionally implement the SEC Functional Group of the P3 Access profile AMH12/AMH14, for security class S0.	A-2-P2				X	
<b>B.2.3.4 P7 Access</b>							
[AMHS-AMU-B10]	A UA supporting P7 access shall conform to the profile in Appendix B Annex H, or Appendix B Annex I of ICAO EUR Doc 020 [8].	A-2-P2				X	
[AMHS-AMU-B11]	A UA supporting P7 access shall conform to the profile in Appendix B Annex D, or Appendix B Annex E of ICAO EUR Doc 020 [8], with the addition of support of the DIR Functional Group as specified in ICAO Doc 9880 Part IIB [5] section 3.1.4.3.1.	A-2-P2				X	
[AMHS-AMU-B12]	It is recommended that a UA supporting P7 access should conform to the Enhanced MS Access profile AMH24.	A-2-P2				X	
[AMHS-AMU-B13]	A UA supporting P7 access should additionally implement the SEC Functional Group of the IPM P7 Access profile AMH24/AMH26, for security class S0 (only).	A-2-P2				X	
[AMHS-AMU-B14]	A UA supporting P7 access shall additionally implement the BC Functional Group of the IPM P7 Access profile AMH24/AMH26 as specified in ICAO Doc 9880 Part IIB [5], section 3.1.4.3.1, for the IPM heading fields indicated as “m” in Table B-1.	A-2-P2				X	
<b>B.2.3.5 Directory Access</b>							
[AMHS-AMU-B15]	An ATS Message User Agent implementing the DIR functional group shall include a DUA for access to the ATN Directory.	A-2-P2				X	
<b>B.2.4 ATS Message Server Requirements</b>							
<b>B.2.4.1 General</b>							
<b>B.2.4.2 MS Access to MTA</b>							
[AMHS-MST-B01]	An MS which supports P3 access in an ATS Message Server supporting the Extended ATSMHS shall conform to the profile in Appendix B Annex G of ICAO EUR Doc 020 [8].	A-2-P2				X	
[AMHS-MST-B02]	An MS which supports P3 access in an ATS Message Server supporting the Extended ATSMHS shall conform to the profile in Appendix B Annex C of ICAO EUR Doc 020 [8], with the addition of support of the DIR Functional Group as specified in ICAO Doc 9880 Part IIB [5], section 3.2.4.3.	A-2-P2				X	
[AMHS-MST-B03]	It is recommended that an MS supporting P3 access should conform to the MTS Access profile AMH23.	A-2-P2				X	
[AMHS-MST-B04]	An MS which supports P3 access should additionally implement the SEC Functional Group of the IPM P3 Access profile AMH23/AMH25, for security class S0.	A-2-P2				X	

Requirement Reference	Requirement Description	Essential Requirements Reference	Test	Demo	Eval	Audit	Notes
[AMHS-MST-B05]	An MS which accesses the MTA by local means shall provide equivalent message submission and delivery functionality to that specified in the P3 access profile above.	A-2-P2				X	
<b>B.2.4.3 P7 Access</b>							
[AMHS-MST-B06]	An MS in an ATS Message Server supporting the Extended ATSMHS shall conform to the P7 access profile in Appendix B Annex H, or Appendix B Annex I of ICAO EUR Doc 020 [8] for message retrieval and indirect submission.	A-2-P2				X	
[AMHS-MST-B07]	An MS in an ATS Message Server supporting the Extended ATSMHS shall conform to the profile in Appendix B Annex D, or Appendix B Annex E of ICAO EUR Doc 020 [8], with the addition of support of the DIR Functional Group as specified in ICAO Doc 9880 Part IIB [5], section 3.1.4.3.1.	A-2-P2				X	
[AMHS-MST-B08]	An MS in an ATS Message Server supporting the Extended ATSMHS should additionally implement the SEC Functional Group of the IPM P7 Access profile AMH24/AMH26, for security class S0 (only).	A-2-P2				X	
[AMHS-MST-B09]	An MS in an ATS Message Server supporting the Extended ATSMHS shall additionally implement the BC Functional Group of the IPM P7 Access profile AMH24/AMH26 as specified in ICAO Doc 9880 Part IIB [5], section 3.1.4.3.1 for the IPM heading fields indicated as “m” in Table B-1.	A-2-P2				X	
<b>B.2.5 ATS Message Server Requirements</b>							
<b>B.2.5.1 General</b>							
<b>B.2.5.2 Directory Access</b>							
[AMHS-GWY-B01]	An AFTN/AMHS Gateway implementing the DIR functional group shall include a DUA for access to the ATN Directory.	A-2-P2				X	
[AMHS-GWY-B02]	It is recommended that the DUA in an AFTN/AMHS Gateway supporting the Extended ATSMHS should be used to retrieve information in support of address and content conversion.	A-2-P2				X	
<b>B.3 CONFORMITY ASSESSMENT MATERIALS</b>							
<b>B.3.1 Compliance Statement</b>							
[AMHS-CA-B01]	A claim of conformance for an implementation shall be supported by completion of the relevant Protocol Implementation Conformance Statement (PICS) pro forma.	A-1-P1, Annex IV-P4				X	Part of Technical File
[AMHS-CA-B02]	Implementers claiming conformance to the specified services shall complete the PICS specified in Appendix B Annex Q of ICAO EUR Doc 020 [8], taking due account of the specific requirements for implementations of AMHS End Systems supporting the Extended ATSMHS specified in this Annex of the EUROCONTROL Specification.	A-1-P1, Annex IV-P4				X	Part of Technical File

Requirement Reference	Requirement Description	Essential Requirements Reference	Test	Demo	Eval	Audit	Notes
[AMHS-CA-B03]	Implementers shall state whether all of the requirements and which of the optional elements of the AFTN/AMHS Gateway supporting the Extended ATSMHS as specified in ICAO Doc 9880 Part IIB [5] section 4 have been implemented, using the pro forma tables in this section or equivalent.	A-1-P1, Annex IV-P4				X	Part of Technical File
[AMHS-CA-B04]	For AFTN/AMHS Gateway implementations, a PICS shall be provided stating the level of support, for each of the elements relevant to support of the Extended ATSMHS, listed in the profile requirements lists in section 4 of ICAO Doc 9880 Part IIB [5] and specified in Table B-3.	A-1-P1, Annex IV-P4				X	Part of Technical File
[AMHS-CA-B05]	AMHS End Systems supporting the Extended ATSMHS shall be tested according to suitable test cases and procedures ensuring adequate coverage of the IHE, FTBP and DIR functional groups.	A-1-P1, Annex IV-P4				X	Part of Technical File
[AMHS-CA-B06]	Testing shall be conducted within a common framework consistent with the procedures in ICAO EUR Doc 020 [8] using appropriate test tools and procedures.	A-1-P1, Annex IV-P4				X	Part of Technical File

### A1.3.3 Annex C – Directory Service

Table 5: Annex C – Directory Service

Requirement Reference	Requirement Description	Essential Requirements Reference	Test	Demo	Eval	Audit	Notes
<b>C.2 REQUIREMENTS AND EXPLANATORY MATERIALS</b>							
<b>C.2.1 General Directory Requirements</b>							
[AMHS-DIR-C01]	AMHS End Systems supporting the DIR functional group shall include access to directory information as specified in the schema defined in ICAO Doc 9880 Part IVA [7].	A-2-P1, A-2-P2				X	
[AMHS-DIR-C02]	The directory functionality shall comply with the standards and ISPs referenced from ICAO Doc 9880 Part IVA [7]	A-2-P1, A-2-P2				X	
[AMHS-DIR-C03]	Directory protocols shall operate over the TCP transport service as specified in ICAO Doc 9880 Part IVA [7], section 5.7.6.3..	B-4.2-P1	X				
<b>C.2.1.1 Architecture</b>							
[AMHS-DIR-C04]	In order to guarantee the consistency of the shared part(s) of the DIT, it shall be ensured that each DSA: a) has a common view of the schema for the shared data, b) supports a common means of directory replication and/or chaining / referral of queries, c) does not require any modification of the data replicated from other DSAs.	A-1-P1				X	

Requirement Reference	Requirement Description	Essential Requirements Reference	Test	Demo	Eval	Audit	Notes
[AMHS-DIR-C05]	The DSA shall implement DSP to support the exchange of data with other DSAs.	B-4.2-P1	X				
[AMHS-DIR-C06]	The DSA should implement DISP including support for incremental and full shadow updates, supplier and consumer initiated, scheduled and on-change updates, attribute filtering and chop shadowing.	B-4.2-P1	X				
[AMHS-DIR-C07]	The DSA shall support the bind operation using as a minimum simple authentication for DAP, DSP and DISP as defined in the base standards.	B-4.2-P1, A-3-P5	X				
[AMHS-DIR-C08]	The DSA should additionally support the bind operation using strong authentication for DAP, DSP and DISP as defined in the base standards.	B-4.2-P1, A-3-P5	X				
[AMHS-DIR-C09]	The Directory service implementation shall allow additional directory object classes and attributes to be included in order to allow the use of this service by other applications within the scope of other private or EATMN directory service deployment.	A-2-P1			X		
[AMHS-DIR-C10]	The DSA shall have the ability to export and import directory information in Lightweight Directory Access Protocol Interchange Format (LDIF) format, where applicable.	B-4.2-P1	X				
<b>C.2.1.2 Directory User Agent access</b>							
[AMHS-DIR-C11]	The DSA shall implement DAP to support user access to the directory information.	B-4.2-P1	X				
[AMHS-DIR-C12]	The DSA may also implement other access protocols based on LDAP [39] or a proprietary protocol to support user access to the directory information.	A-2-P1			X		
[AMHS-DIR-C13]	If DAP or LDAP is implemented by the DUA, the use of "referral" identifying a DSA external to the EATMN should be strictly controlled.	A-2-P1			X		
<b>C.2.1.3 Directory Contents Access Policy</b>							
[AMHS-DIR-C14]	It shall be possible to define access control policy in order to regulate what type of operation can be performed on a directory entry, attributes or values.	A-2-P1, A-3-P5			X		
[AMHS-DIR-C15]	The basic operations listed in Table C-1 shall be supported by DUAs and DSAs.	B-4.2-P1	X				
<b>C.2.2 AMHS-Specific Directory Requirements</b>							
<b>C.2.2.1 Directory Functions in support of AMHS</b>							
[AMHS-DIR-C16]	The Directory implementation shall support the following functions: a) Name resolution b) Distribution list (DL) expansion and management c) Determination of recipient (direct/indirect DUA or DL) capabilities d) AFTN/AMHS address conversion and publication	B-4.2-P1	X				
[AMHS-DIR-C17]	The Directory implementation should additionally support the following function, if required: e) Retrieval of security certificates and CRLs	B-4.2-P1	X				

Requirement Reference	Requirement Description	Essential Requirements Reference	Test	Demo	Eval	Audit	Notes
[AMHS-DIR-C18]	The Directory implementation may additionally support one or more of the following functions: f) Support for system configuration g) AMHS systems management information h) Address book	B-4.2-P1	X				
[AMHS-DIR-C19]	AMHS End System support of the directory functions shall be as indicated in Table C-2	B-4.2-P1	X				
<b>C.2.2.2 Directory Information in support of AMHS</b>							
[AMHS-DIR-C20]	The Directory information tree exported by Border DSAs shall conform to the DIT structure defined in ICAO Doc 9880 Part IVA [7], unless otherwise stated in this section.	B-4.2-P1	X				
[AMHS-DIR-C22]	It is recommended that the DSA should export only <i>atn-amhs-user</i> and <i>atn-amhs-distribution-list</i> object-classes for users which have the capability to send/receive AMHS messages to/from other ATSMHS users.	B-4.2-P1			X		
[AMHS-DIR-C23]	It is recommended that the exported / imported sub-trees should be attached to the country root DIT.	B-4.2-P1	X				
[AMHS-DIR-C24]	The DSA shall use this DIT structure to support the name resolution function, using <i>Country</i> , <i>Organization</i> , <i>atn-organization</i> and <i>atn-amhs-user</i> object-classes.	B-4.2-P1	X				
[AMHS-DIR-C25]	The DSA shall use this DIT structure to support the DL expansion and management function, with MTAs accessing members of the <i>atn-amhs-distribution-list</i> object-class.	B-4.2-P1	X				
[AMHS-DIR-C26]	The DSA shall use this DIT structure to support the AFTN/AMHS address conversion function performed by the AFTN/AMHS Gateway based on the “Simple AMHS address conversion directory algorithm” described below, using object classes <i>Country</i> , <i>Organization</i> , <i>atn-organization</i> , <i>atn-amhs-user</i> , <i>atn-amhs-distribution-list</i> and <i>atn-amhsMD</i> .	B-4.2-P1	X				
[AMHS-DIR-C27]	The attribute <i>description</i> of the object classes <i>Country</i> and <i>Organization</i> used as the root of the exported sub-tree shall be used as follows to store the current version of this sub-tree: Format of the <i>description</i> attribute: “<version number> - <description of the object>”.	B-4.2-P1	X				
[AMHS-DIR-C28]	The country or the organization shall maintain the version of its exported sub-tree.	A-1-P1				X	
<b>C.2.2.3 Simple AMHS Address Conversion Directory Algorithm</b>							

Requirement Reference	Requirement Description	Essential Requirements Reference	Test	Demo	Eval	Audit	Notes
[AMHS-DIR-C29]	Each DSA shall include: a) the subtree for its own ANSP containing local AMHS user information relative to AFTN/AMHS address translation, b) the MD-registry sub tree starting with a member of the <i>organization</i> object-class named O=ICAO-MD-Registry and containing <i>atn-amhsMD</i> objects (ideally replicated from a master DSA managed by ICAO), c) a replicated sub tree or a reference to the other ANSP exported DIT.	B-4.2-P1			X		
[AMHS-DIR-C30]	The Directory information shall support address conversion between AMHS and AFTN address types.	B-4.2-P1	X				
[AMHS-DIR-C31]	An O/R Address (MF-Address) included in an AMHS message shall be processed for translation into the AFTN address in one of four mutually exclusive manners, depending on the MF-Address format, after preliminary conversion of all address attribute values to upper case characters:	B-4.2-P1	X				
[AMHS-DIR-C32]	For AFTN to AMHS address conversion, the following algorithm shall be supported:	B-4.2-P1	X				
[AMHS-DIR-C33]	States supporting the CAAS scheme within the EATMN should register values of the "Organization Name" field with length not exceeding 8 characters.	A-2-P1				X	
<b>C.2.3 Directory support of PKI</b>							
[AMHS-DIR-C34]	When being used to provide Directory support for PKI, the DSA shall use the specified DIT structure to provide support for retrieval of security certificates and CRLs, using <i>atn-amhs-user</i> (attribute <i>atn-der-certificate</i> ) and <i>atn-certification-authority</i> object-classes.	A-2-P1, A-3-P5	X				
<b>C.2.4 System capacity and performance</b>							
[AMHS-DIR-C35]	The DSA design should be scalable in a cost effective manner in order to be able to store more AMHS information and support additional DUA directory operations.	A-2-P1				X	
<b>C.3 CONFORMITY ASSESSMENT MATERIALS</b>							
<b>C.3.1 Object Class Requirements</b>							
[AMHS-CA-C01]	DSAs shall implement as a minimum the object classes specified in Table C-3 to Table C-6, in order to guarantee correct understanding of the data shared between DMDs	B-4.2-P1	X				
<b>C.3.2 Attribute Requirement</b>							
[AMHS-CA-C02]	Table C-7 specifies the attributes that shall be used in support of the ATS Message Handling Service for each required object class.	B-4.2-P1	X				
<b>C.3.3 List of X.500 Global Statement and Protocol Operations Supported by the Directory Service</b>							
[AMHS-CA-C03]	Table C-8 specifies the overall conformance and protocol operations that shall be used in support of the ATS Message Handling Service for each mandatory object class.	B-4.2-P1			X		

Requirement Reference	Requirement Description	Essential Requirements Reference	Test	Demo	Eval	Audit	Notes
<b>C.3.4 Requirements statement for DUAs</b>							
[AMHS-CA-C04]	Implementers shall state whether all of the requirements and which of the optional elements of the DUA supporting the Extended ATSMHS, as specified in ICAO Doc 9880 Part IVA [7] section 5.2.1, have been implemented, using the table in this section or equivalent.	B-4.2-P1			X		
<b>C.3.5 Requirements statement for DSAs</b>							
[AMHS-CA-C05]	Implementers shall state whether all of the requirements and which of the optional elements of the DSA supporting the Extended ATSMHS, as specified in ICAO Doc 9880 Part IVA [7] section 5, have been implemented, using the table in this section or equivalent.	B-4.2-P1			X		
<b>C.3.6 Requirements statement for Conformance by a Shadow Supplier</b>							
[AMHS-CA-C06]	For a DSA supporting the directory information shadowing protocol, implementers shall state whether all of the requirements and which of the optional elements of the DSA supporting the Extended ATSMHS, as specified in ICAO Doc 9880 Part IVA [7] section 5.5, have been implemented, using the table in this section or equivalent.	B-4.2-P1			X		
<b>C.3.7 Requirements statement for Conformance by a Shadow Consumer</b>							
[AMHS-CA-C07]	For a DSA supporting the directory information shadowing protocol, implementers shall state whether all of the requirements and which of the optional elements of the DSA supporting the Extended ATSMHS, as specified in ICAO Doc 9880 Part IVA [7] section 5.5, have been implemented, using the table in this section or equivalent.	B-4.2-P1			X		

### A1.3.4 Annex D – Security

Table 6: Annex D – Security

Requirement Reference	Requirement Description	Essential Requirements Reference	Test	Demo	Eval	Audit	Notes
<b>D.2 REQUIREMENTS AND EXPLANATORY MATERIALS</b>							
<b>D.2.1 Introduction</b>							
<b>D.2.2 General Requirements</b>							
<i>D.2.2.1 Security Architecture</i>							
[AMHS-SEC-D01]	An AMHS End System implementation shall implement protocol provisions as necessary to comply with the local security policy relating to aeronautical data access and interchange.	A-3-P3, A-3-P5				X	



Requirement Reference	Requirement Description	Essential Requirements Reference	Test	Demo	Eval	Audit	Notes
[AMHS-SEC-D02]	Measures should be taken by ANSPs and other entities providing data communications services to ensure appropriate security of information exchanges	A-3-P1				X	
[AMHS-SEC-D04]	Implementations shall be conformant with the Extended ATSMHS and in particular the security aspects of ATN relevant for ground-ground communication; Chapter 8.3.1.1 (Framework Standards) of the ATN Security provisions [6] is fully applicable.	A-3-P5				X	
[AMHS-SEC-D05]	Each State implementing AMHS Security shall designate a Trusted Third Party (TTP) acting as a Root Certificate Authority (CA) which issues certificates and certificate revocation lists (CRLs), in accordance with chapter 8.3.1.2.2 of the ATN Security provisions [6]	A-3-P5				X	
[AMHS-SEC-D06]	The TTP shall conform to the ETSI Guide EG 201 057 [13], which defines the role and attribution of a TTP acting as a CA in a PKI.	A-3-P5				X	
[AMHS-SEC-D07]	Item 8.3.1.2.3 of the ATN Security provisions [6] shall be applicable in the conditions provided below.	A-3-P5				X	
[AMHS-SEC-D08]	CAs in the EATMN shall use policies to ensure the overall security of the ATN.	A-3-P5				X	
[AMHS-SEC-D09]	CAs shall be conformant with Directive 1999/93/EC [2], which defines a Community framework for electronic signatures.	A-3-P5				X	
[AMHS-SEC-D10]	CAs shall comply with the certificate policy requirements defined in ETSI specification TS 101 456 [14]	A-3-P5				X	
[AMHS-SEC-D11]	Where the ATN Security provisions [6] in section 8.4 refer to RFC 2527, this shall be replaced with a reference to RFC 3647 [21]	A-3-P5				X	
[AMHS-SEC-D12]	CAs shall develop a Certificate Policy (CP) that defines the creation, management, and use of public key certificates that they issue, consistent with section 8.4.1.1 of the ATN Security provisions [6]	A-3-P5				X	
[AMHS-SEC-D13]	CAs shall publish a Certificate Practice Statement (CPS) that describes the expected use of public key certificates that they issue, consistent with section 8.4.2.1 of the ATN Security provisions [6]	A-3-P5				X	
[AMHS-SEC-D14]	The CP and CPS shall be aligned with the framework presented in RFC 3647 [21].	A-3-P5				X	
[AMHS-SEC-D15]	Each CA shall define its own CPS conformant with the rules defined in ETSI TS 101 456 [14].	A-3-P5				X	
[AMHS-SEC-D16]	Each CA shall propose a service for certificate and CRL distribution.	A-3-P5				X	
[AMHS-SEC-D17]	Each CA shall give simple access to the public certificate and CRL repository in its own domain.	A-3-P5	X				
[AMHS-SEC-D18]	The distribution system of public key certificates and CRLs should be done using Directory services.	A-3-P5	X				

Requirement Reference	Requirement Description	Essential Requirements Reference	Test	Demo	Eval	Audit	Notes
[AMHS-SEC-D19]	According to item 8.3.1.2.7 of the ATN Security provisions [6] “If a directory service is used for certificate and CRL distribution, the service shall conform to the ATN directory service as specified in [...ICAO Doc 9880 Part IVA [7]]”. This shall be taken to mean conformity with the Directory as specified in Annex C of this EUROCONTROL Specification.	A-3-P5				X	
<b>D.2.2.2 Cryptographic and Hashing functions</b>							
[AMHS-SEC-D20]	The EATMN PKI in support of AMHS should therefore be based on a common ATS Bridge CA (see Figure C-2) in order to: a) Simplify the process of cross-certification for each CA; b) Minimise the issues due to multiple policy agreements; c) Minimise the risk of problems occurring due to the limit of validity of cross certificates; d) Allow a central organisation to verify that the policy applied by each CA complies with the European directive on a Community framework for electronic signatures [2].	A-3-P5				X	
[AMHS-SEC-D21]	The cryptographic signing and hashing functions and parameter settings shall be conformant with ATN Security provisions [6] Chapter 8.5.	A-3-P5				X	
[AMHS-SEC-D22]	The general certificate format used for ATN PKI certificates shall be conformant with the X.509 Format with parameters defined in chapter 8.4.3 of the ATN Security provisions [6]	A-3-P5			X		
[AMHS-SEC-D23]	The signature scheme E-ATSMHS-SEC shall be conformant, for the hash function, to the Secure Hash Standard (SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512) defined in FIPS 180-2: Secure Hash Standard (SHS) [15].	A-3-P5				X	
[AMHS-SEC-D24]	The elements of a certificate should be encoded following the DER (Distinguished Encoding Rules) standard defined in the ITU-T Rec X.509 (section 8.7) and specified by the ITU-T Rec X.690 [36].	A-3-P5	X				
[AMHS-SEC-D25]	It is recommended that a symmetric algorithm should be used for the Content Integrity Check algorithm in Extended ATSMHS, and that this should initially be the secure hash algorithm “SHA-1”.	A-3-P5				X	
<b>D.2.3 AMHS Security Specific Requirements</b>							
<b>D.2.3.1 Security Policy</b>							
[AMHS-SEC-D26]	If secure messaging is required in the Extended ATSMHS, a general AMHS end-to-end security policy shall be implemented in compliance with ICAO Doc 9880 Part IIB [5] section 2.2.3, providing the following security services: a) Message origin authentication; and b) Content integrity.	A-3-P5	X				

Requirement Reference	Requirement Description	Essential Requirements Reference	Test	Demo	Eval	Audit	Notes
[AMHS-SEC-D27]	An appropriate security policy shall be implemented in order to secure the AMHS, notably by applying common security rules to protect the distributed physical resources supporting message submission, transfer and delivery.	A-3-P5				X	
[AMHS-SEC-D28]	For messages using these security services, the processing of the message envelope shall be in compliance with ICAO Doc 9880 Part IIB [5] sections 3.1.4.3 and 3.2.4.	A-3-P5	X				
<i>D.2.3.2 AMHS Security Framework</i>							
[AMHS-SEC-D29]	The Security model given in §2.2.3 of the AMHS technical provisions in ICAO Doc 9880 Part IIB [5] shall be applied.	A-3-P5				X	
[AMHS-SEC-D30]	The general AMHS security policy shall be aligned with the general ATN Security Framework as defined in the ATN Security provisions [6] this is a common minimum which does not prevent specific communities of AMHS users from implementing more stringent security policies in case of additional user requirements.	A-3-P5				X	
[AMHS-SEC-D31]	The use of AMHS security services shall apply to: a) communications between direct AMHS users supporting the Extended ATSMHS; and b) communications from direct AMHS users to indirect AMHS users as far as the AFTN/AMHS Gateway supporting the Extended ATSMHS.	A-3-P5			X		
[AMHS-SEC-D32]	The AMHS security policy shall make use of the Elliptic Curve Digital Signature Algorithm (ECDSA) as specified in the ATN Security provisions [6] section 8.5.5.	A-3-P5				X	
[AMHS-SEC-D33]	For the support of security in the context of the Extended ATSMHS, an ATS Message User Agent shall implement the Security requirements defined in §3.1.4.3.2 of ICAO Doc 9880 Part IIB [5]	A-3-P5				X	
[AMHS-SEC-D34]	The generation by the ATS Message User Agent of the message token in the per-recipient-extensions of the message envelope shall be as specified in section 3.1.4.3.2.2.1 of ICAO Doc 9880 Part IIB [5] refined as specified in this Annex.	A-3-P5	X				
[AMHS-SEC-D35]	For the support of security in the context of the Extended ATSMHS, an MTA in an ATS Message Server shall implement the requirements for the support by an MTA of the SEC Functional Group, implementing Security-Class S0, as defined in §3.2.4.3 b) of ICAO Doc 9880 Part IIB [5]	A-3-P5	X				
[AMHS-SEC-D36]	For the support of security in the context of the Extended ATSMHS, a Message Store in an ATS Message Server shall implement the requirements for the support by an MS of the SEC Functional Group, implementing Security-Class S0, as defined in §3.2.4.4 b) of ICAO Doc 9880 Part IIB [5]	A-3-P5	X				

Requirement Reference	Requirement Description	Essential Requirements Reference	Test	Demo	Eval	Audit	Notes
[AMHS-SEC-D37]	For the support of security in the context of the Extended ATSMHS, an AFTN/AMHS Gateway shall implement the requirements for handling the security-related elements of the message transfer envelope as defined in §4.5.2.4.12 to 4.5.2.4.16 of ICAO Doc 9880 Part IIB [5]	A-3-P5	X				
[AMHS-SEC-D38]	It is recommended that to simplify certificate signature checking, and facilitate interoperability, the certificate (and CRL) extensions that may be used within the Extended ATSMHS are precisely defined and kept to a minimum.	A-3-P5				X	
<i>D.2.3.3 Recommendations for Secure Message Submission</i>							
[AMHS-SEC-D39]	A message originator wishing to send a secure message at an ATS Message User Agent that supports AMHS SEC shall create and sign a message-token for each recipient in the per-recipient-extensions in the message envelope.	A-3-P5	X				
[AMHS-SEC-D40]	The MessageTokenSignedData should include only the CIC algorithm identifier and the CIC value, computed using a symmetric algorithm.	A-3-P5	X				
[AMHS-SEC-D41]	It is recommended that message originators using AMHS Security should provide a valid certificate containing the required public key in the <i>originators-certificate</i> element in the message envelope extensions.	A-3-P5	X				
[AMHS-SEC-D42]	It is recommended that use of the <i>multiple-originator-certificates</i> element in the message envelope extensions should be prohibited on message submission.	A-3-P5	X				
<i>D.2.3.4 Recommendations for Secure Message Reception</i>							
[AMHS-SEC-D43]	It is recommended that on receipt of a message containing the originator's certificate in the message envelope extensions, the originator's O/R Address should be compared with one found in the <i>Subject Alternative Name</i> extension of the certificate to ensure that the supplied certificate is associated with the message originator.	A-3-P5	X				
[AMHS-SEC-D44]	It is recommended that an OCSP Responder compliant with RFC 2560 [41] should be deployed to facilitate the verification of received certificates.	A-3-P5			X		

Requirement Reference	Requirement Description	Essential Requirements Reference	Test	Demo	Eval	Audit	Notes
[AMHS-SEC-D45]	An application should validate the message token, contained in the message delivery envelope extensions, when the message is first received, including: a) Verifying the time field in the message token; b) Applying the CIC Algorithm Id to the received message content / stated algorithm id, and comparing this to the received CIC Hash value; c) Applying the Signature Algorithm Id and originator's certificate public key to the whole contents of the Asymmetric Token, and comparing this with the token signature; d) Checking the Recipient Name in the message-token.	A-3-P5	X				
[AMHS-SEC-D46]	A receiving application should report an error if a message-token that is 'too old' is received (except when displaying an archived message).	A-3-P5	X				
[AMHS-SEC-D47]	The maximum acceptable time difference between the time field in the message token and the current system time should be specified in the security policy.	A-3-P5				X	
[AMHS-SEC-D48]	If a message is received that is too old, the receiving application should check the message integrity but ignore the signature.	A-3-P5	X				
[AMHS-SEC-D49]	When applying the CIC Algorithm Id to the received message content / stated algorithm id, and comparing this to the received CIC Hash, it is recommended that the AMHS SEC convention is to use the message content as received, i.e. the recipient should not need to ensure that it is DER-encoded.	A-3-P5			X		
<i>D.2.3.5 Message Sequence Integrity</i>							
[AMHS-SEC-D50]	Message sequence integrity should be achieved by the message originator setting the Time field in the Message Token to the current time, and the message recipient checking that the value of this field is within acceptable parameters.	A-3-P5	X				
[AMHS-SEC-D51]	Message sequence integrity may be provided as claimed in ISO/IEC 10021-4 [18]. In an AMHS End System supporting the Extended ATSMHS, the message-sequence-number may be present in the asymmetric token <i>MessageTokenSignedData</i> . As stated in ISO/IEC 10021-4, the first occurrence of a message sequence number can be a random number.	A-3-P5	X				
[AMHS-SEC-D52]	However, it is recommended that applications using the Extended ATSMHS should avoid using the message-sequence-number field in the Message Token for message sequence integrity assurance.	A-3-P5			X		

Requirement Reference	Requirement Description	Essential Requirements Reference	Test	Demo	Eval	Audit	Notes
<b>D.3 CONFORMITY ASSESSMENT MATERIALS</b>							
[AMHS-CA-D01]	For ATS Message User Agent implementations supporting the SEC functional group, a PICS shall be provided stating the level of support, for each of the elements listed in the profile requirements list in Table 3-3 of ICAO Doc 9880 Part IIB [5].	B-4.2-P1	X				
[AMHS-CA-D02]	Support for message-sequence-number in the message token signed-data, which is indicated as “Optional” in the referenced PRL, should be made “M” (Mandatory), to allow for the possible provision of the Message Sequence Integrity function.	B-4.2-P1	X				
[AMHS-CA-D03]	Support for the encrypted-data and content-confidentiality-algorithm-id fields in the message token, which is indicated as “Optional” in the referenced PRL, should be considered “out of scope”, and not used when communicating with AMHS users compliant with this EUROCONTROL Specification, since the AMHS security model in ICAO Doc 9880 Part IIB [5], does not include message confidentiality.	B-4.2-P1	X				
<b>APPENDIX 1 TO ANNEX D</b>							
<b>PDR Resolutions Applicable to ICAO Doc 9705, Third Edition, Sub-Volume VIII</b>							

Requirement Reference	Requirement Description	Essential Requirements Reference	Test	Demo	Eval	Audit	Notes																																										
[AMHS-SEC-D54]	<p>Security implementations shall include the relevant PDR resolutions from the following list:</p> <table border="1" data-bbox="434 341 1225 1117"> <thead> <tr> <th data-bbox="434 341 589 368">PDR ref</th> <th data-bbox="589 341 1225 368">Title</th> </tr> </thead> <tbody> <tr> <td data-bbox="434 368 589 427">M1030007</td> <td data-bbox="589 368 1225 427">Security - Editorial errors found during development of Guidance Material</td> </tr> <tr> <td data-bbox="434 427 589 486">M1030008</td> <td data-bbox="589 427 1225 486">Security - Defects found during development of Guidance Material</td> </tr> <tr> <td data-bbox="434 486 589 545">M2030004</td> <td data-bbox="589 486 1225 545">All SV - Editorials (version of PDR current on 2004/05/28)</td> </tr> <tr> <td data-bbox="434 545 589 572">M2080001</td> <td data-bbox="589 545 1225 572">SV8 - Unnecessary random challenge field</td> </tr> <tr> <td data-bbox="434 572 589 632">M2080003</td> <td data-bbox="589 572 1225 632">Security - Clarify representation of AMHS identities in ATN certificates</td> </tr> <tr> <td data-bbox="434 632 589 659">M2080004</td> <td data-bbox="589 632 1225 659">Security - Additional extensions in CA certificates</td> </tr> <tr> <td data-bbox="434 659 589 686">M2080005</td> <td data-bbox="589 659 1225 686">Security - Clarify ATN CRL processing</td> </tr> <tr> <td data-bbox="434 686 589 745">M2080006</td> <td data-bbox="589 686 1225 745">Security - Add warning concerning the use of invalid keys by the secret value derivation primitive</td> </tr> <tr> <td data-bbox="434 745 589 772">M2080007</td> <td data-bbox="589 745 1225 772">Security - Remove CheckResult references from 8.6.3</td> </tr> <tr> <td data-bbox="434 772 589 831">M2080008</td> <td data-bbox="589 772 1225 831">Security - Remove duplicate certificate retrieval requirements</td> </tr> <tr> <td data-bbox="434 831 589 858">M2080009</td> <td data-bbox="589 831 1225 858">Security - Sub-Volume VIII ASN.1</td> </tr> <tr> <td data-bbox="434 858 589 885">M2090002</td> <td data-bbox="589 858 1225 885">SV8, SV4 - SSO-GetCertificatePath target</td> </tr> <tr> <td data-bbox="434 885 589 912">M2090003</td> <td data-bbox="589 885 1225 912">SV8 - ASN.1 padding issues</td> </tr> <tr> <td data-bbox="434 912 589 940">M2090004</td> <td data-bbox="589 912 1225 940">SV8 - SSO-SessionKey Certificate Knowledge</td> </tr> <tr> <td data-bbox="434 940 589 967">M2090005</td> <td data-bbox="589 940 1225 967">SV8 - SSO counter initialization</td> </tr> <tr> <td data-bbox="434 967 589 994">M2100005</td> <td data-bbox="589 967 1225 994">SV8 - Tagging in SV8 ASN.1 module</td> </tr> <tr> <td data-bbox="434 994 589 1021">M4020001</td> <td data-bbox="589 994 1225 1021">Security - Error in ATN Key Derivation Function</td> </tr> <tr> <td data-bbox="434 1021 589 1048">M4030001</td> <td data-bbox="589 1021 1225 1048">SV8 - Missing requirement on User Data padding</td> </tr> <tr> <td data-bbox="434 1048 589 1075">M4050007</td> <td data-bbox="589 1048 1225 1075">SV8 - Key lifetime clarification</td> </tr> <tr> <td data-bbox="434 1075 589 1102">M6080004</td> <td data-bbox="589 1075 1225 1102">SV8 - Directory Security Requirements</td> </tr> </tbody> </table>	PDR ref	Title	M1030007	Security - Editorial errors found during development of Guidance Material	M1030008	Security - Defects found during development of Guidance Material	M2030004	All SV - Editorials (version of PDR current on 2004/05/28)	M2080001	SV8 - Unnecessary random challenge field	M2080003	Security - Clarify representation of AMHS identities in ATN certificates	M2080004	Security - Additional extensions in CA certificates	M2080005	Security - Clarify ATN CRL processing	M2080006	Security - Add warning concerning the use of invalid keys by the secret value derivation primitive	M2080007	Security - Remove CheckResult references from 8.6.3	M2080008	Security - Remove duplicate certificate retrieval requirements	M2080009	Security - Sub-Volume VIII ASN.1	M2090002	SV8, SV4 - SSO-GetCertificatePath target	M2090003	SV8 - ASN.1 padding issues	M2090004	SV8 - SSO-SessionKey Certificate Knowledge	M2090005	SV8 - SSO counter initialization	M2100005	SV8 - Tagging in SV8 ASN.1 module	M4020001	Security - Error in ATN Key Derivation Function	M4030001	SV8 - Missing requirement on User Data padding	M4050007	SV8 - Key lifetime clarification	M6080004	SV8 - Directory Security Requirements	A-3-P5				X	
PDR ref	Title																																																
M1030007	Security - Editorial errors found during development of Guidance Material																																																
M1030008	Security - Defects found during development of Guidance Material																																																
M2030004	All SV - Editorials (version of PDR current on 2004/05/28)																																																
M2080001	SV8 - Unnecessary random challenge field																																																
M2080003	Security - Clarify representation of AMHS identities in ATN certificates																																																
M2080004	Security - Additional extensions in CA certificates																																																
M2080005	Security - Clarify ATN CRL processing																																																
M2080006	Security - Add warning concerning the use of invalid keys by the secret value derivation primitive																																																
M2080007	Security - Remove CheckResult references from 8.6.3																																																
M2080008	Security - Remove duplicate certificate retrieval requirements																																																
M2080009	Security - Sub-Volume VIII ASN.1																																																
M2090002	SV8, SV4 - SSO-GetCertificatePath target																																																
M2090003	SV8 - ASN.1 padding issues																																																
M2090004	SV8 - SSO-SessionKey Certificate Knowledge																																																
M2090005	SV8 - SSO counter initialization																																																
M2100005	SV8 - Tagging in SV8 ASN.1 module																																																
M4020001	Security - Error in ATN Key Derivation Function																																																
M4030001	SV8 - Missing requirement on User Data padding																																																
M4050007	SV8 - Key lifetime clarification																																																
M6080004	SV8 - Directory Security Requirements																																																

**EUROCONTROL Specification on the Air Traffic Services Message Handling System (AMHS)**

**Appendix 2**

**Current Editions of Referenced ISO/IEC Standards and IETF RFCs**

**TABLE OF CONTENTS**

Appendix 2. Current Editions of Referenced Standards.....	2
A2.1 INTRODUCTION.....	2
A2.2 LIST OF REFERENCED STANDARDS.....	2



## APPENDIX 2. CURRENT EDITIONS OF REFERENCED STANDARDS

### A2.1 INTRODUCTION

A2.1.1 This informational Appendix provides references to the current editions of international standards that are invoked in the baseline ICAO detailed technical specifications for the ATS Message Handling Service (ICAO Doc 9880 Part IIB) and the ATN Directory (ICAO Doc 9880 Part IVA), and the EUR AMHS Manual (ICAO EUR Doc 020).

A2.1.2 ICAO Doc 9705 is gradually being superseded by ICAO Doc 9880. It provides in Sub-Volume I, section 1.1.2, a list of referenced standards. This list refers to specific editions of the standards, identified by their year of publication. Other parts of Doc 9705 / Doc 9880 generally make non-specific references to these standards (i.e. without edition number or year of publication), but as stated in Sub-Volume I, they are in fact referring to the specific editions and/or versions listed therein.

A2.1.3 A note in ICAO Doc 9705, section 1.1.2 states:

*"Note 1.— The cited references were used in the preparation of Doc 9705. In the course of the normal progression of ISO and ITU-T standards, new editions are released. New editions to the referenced documents can be safely used in place of the referenced documents with the understanding that new functions introduced in those editions might not be supported by other implementations. Additionally, Amendments to ISO standards are incorporated into the following editions of the base standard and therefore information can be found there."*

A2.1.4 In support of implementers, the table in this Appendix shows the latest editions of the standards used/referenced in the relevant parts of ICAO Doc. 9705 / Doc 9880. The intention is not to mandate their use but to indicate the current standards editions (as at end of 2008). As noted above, these latest editions may be used in place of the referenced editions, provided backwards compatibility is maintained where any new functionality is introduced in later editions.

A2.1.5 In case of doubt, the specific edition referred to in ICAO Doc 9705 / Doc 9880 remains the master reference.

A2.1.6 As some of these editions are now unobtainable, the later edition may be used by implementers, with the above provisos.

### A2.2 LIST OF REFERENCED STANDARDS

A2.2.1 The following table lists the ISO/IEC standards, ITU-T Recommendations and IETF RFCs that are referenced from the AMHS technical provisions in ICAO Doc 9880 Part IIB, the Directory technical provisions in ICAO Doc 9880 Part IVA and the EUR AMHS Manual ICAO EUR Doc 020. In general, these are not qualified by a particular year or edition number, but refer to the list of external standards in Doc 9705/SV1.

A2.2.2 The left hand column gives the reference as given in the ICAO document. The right hand column provides the full title and current status of the standard, as well as a list of withdrawn editions of each standard, taken from the ISO online catalogue at [www.iso.ch](http://www.iso.ch). It also lists the relevant Amendments and Technical Corrigenda to the base standard.

A2.2.3 Implementers are advised to check the latest version of the standards, which often contain technical corrigenda compared with earlier versions.

*Note: ISO/IEC 10021 multi-part standard "Information technology -- Message Handling Systems (MHS)" was originally entitled "Information technology -- Text Communication -- Message-Oriented Text Interchange Systems (MOTIS)".*

**Table 1: Status of Referenced Standards**

Reference in ICAO Document	Title and Current Status
ISO 646 ISO/IEC 646:1991	ISO/IEC 646:1991 Information technology -- ISO 7-bit coded character set for information interchange Edition: 3 (1991)
ISO/IEC 7498-1:1994	ISO/IEC 7498-1:1994 Information technology -- Open Systems Interconnection -- Basic Reference Model: The Basic Model Edition: 2 (1994)
ISO 8649	ISO/IEC 8649:1996 Information technology -- Open Systems Interconnection -- Service definition for the Association Control Service Element Edition: 2 (1996)
ISO 8859-1	ISO/IEC 8859-1:1998 Information technology -- 8-bit single-byte coded graphic character sets -- Part 1: Latin alphabet No. 1 Edition: 1 (1998)
ISO 9072-2.	ISO/IEC 9072-2:1989 Information processing systems -- Text communication -- Remote Operations -- Part 2: Protocol specification Edition: 1 (1989)
ISO 9594-7.	Information technology -- Open Systems Interconnection -- The Directory: Selected object classes Edition: 4 (2001)
ISO/IEC 3166:1993	ISO 3166-1:2006 Codes for the representation of names of countries and their subdivisions -- Part 1: Country codes Edition: 2 (2006) Original single-part std 1993 Ed 4 withdrawn 1997
ISO/IEC 8327-1	ISO/IEC 8327-1:1996 Information technology -- Open Systems Interconnection -- Connection-oriented Session protocol: Protocol specification Edition: 2 (1996)
(ISO/IEC 8327-1:1996/ Cor 1:2002)	Edition: 1 (2002)
ISO/IEC 8822	ISO/IEC 8822:1994 Information technology -- Open Systems Interconnection -- Presentation service definition Edition: 2 (1994)
ISO/IEC 8859-1: 1987	ISO/IEC 8859-1:1998 Information technology -- 8-bit single-byte coded graphic character sets -- Part 1: Latin alphabet No. 1 Edition: 1 (1998) 1987 Ed 1 withdrawn 1998
ISO/IEC 9066-1	ISO/IEC 9066-1:1989 Information processing systems -- Text communication -- Reliable Transfer -- Part 1: Model and service definition Edition: 1 (1989)
ISO/IEC 10021:1990 ISO/IEC 10021:2003	(Generic reference to all parts of ISO/IEC 10021)
ISO/IEC 10021-1:1990 ISO/IEC 10021-1:2003	Information technology -- Message Handling Systems (MHS) -- Part 1: System and service overview Edition 2 (2003) 1990 Ed 1 withdrawn 2003
(ISO/IEC 10021-1/Amd.1:1993)	Message Store Extensions 1994 Ed 1 withdrawn 2003
ISO/IEC 10021-1/ Amd.2:1994.	(Not in ISO catalogue)
ISO/IEC 10021-2 ISO/IEC 10021-2:1990 ISO/IEC 10021-2:2003	Information technology -- Message Handling Systems (MHS): Overall architecture Edition: 3 (2003) 1990 Ed 1 withdrawn 2003; 1996 Ed 2 withdrawn 2003

Reference in ICAO Document	Title and Current Status
ISO/IEC 10021-2/Amd.1:1993.	1994 Ed 1 withdrawn 1996
ISO/IEC 10021-2/Amd.2:1994.	1994 Ed 1 withdrawn 1996
ISO/IEC 10021-3:1990.	Information technology -- Text Communication -- Message-Oriented Text Interchange Systems (MOTIS) -- Part 3: Abstract Service Definition Conventions Edition: 1 1990 Ed 1 withdrawn 1999
ISO/IEC 10021-4:1990 ISO/IEC 10021-4:2003	Information technology -- Message Handling Systems (MHS): Message transfer system -- Abstract service definition and procedures Edition: 3 (2003) 1990 Ed 1 withdrawn 2003; 1997 Ed 2 withdrawn 2003
ISO 10021-4:1997/Cor. 1:1998	1998 Ed 1 withdrawn 2003
ISO/IEC 10021-4 Technical Corrigendum 5.	1995 Ed 1 withdrawn 1997
ISO/IEC 10021-4/Amd.1:1994.	1994 Ed 1 withdrawn 1997
ISO/IEC 10021-5:1990 ISO/IEC 10021-5:1999.	Information technology -- Message Handling Systems (MHS): Message store: Abstract service definition Edition: 4 (1999) 1990 Ed 2 withdrawn 2003; 1994 Ed 1 withdrawn 1996; 1996 Ed 3 withdrawn 2000
ISO/IEC 10021-5/ Amd. 1:199x.	Additional correlation attribute and security error code Edition: 1 (1998) withdrawn 2000
ISO/IEC 10021-6:1990 ISO/IEC 10021-6:2003	Information technology -- Message Handling Systems (MHS): Protocol specifications Edition: 3 (2003) 1990 Ed 1 withdrawn 2003; 1996 Ed 2 withdrawn 2003
(ISO/IEC 10021-6:1996/Amd 1:1998)	Use of ISO/IEC 10646 characters in OR-addresses Edition: 1 withdrawn 2003
ISO/IEC 10021-7:1990 ISO/IEC 10021-7:2003	Information technology -- Message Handling Systems (MHS): Interpersonal messaging system Edition: 3 (2003) 1990 Ed 1 withdrawn 2003; 1997 Ed 2 withdrawn 2003
ISO 10021-7:1997/ Cor. 1:1998.	Ed 1 1998 withdrawn 2003
(ISO/IEC 10021-7:1997/Amd 1:1998)	Security error diagnostic codes Edition: 1 withdrawn 2003
ISO/IEC 10021-10 (1998)	Information technology -- Message Handling Systems (MHS) -- Part 10: MHS routing Edition: 2 (1999) 1998 Ed 1 withdrawn 2000; 1997 Ed 2 withdrawn 2003
ISO/IEC 13248-1	Information technology -- Open Systems Interconnection -- The Directory: Protocol Implementation Conformance Statement (PICS) proforma for the Directory Access Protocol Edition: 1 (1998) withdrawn 2003
ISO/IEC 13248-2	Information technology -- Open Systems Interconnection -- The Directory: Protocol Implementation Conformance Statement (PICS) proforma for the Directory System Protocol Edition: 1 (1998) withdrawn 2003
(ISO/IEC 13248-4)	Information technology -- Open Systems Interconnection -- The Directory: Protocol Implementation Conformance Statement /PICS) proforma for the Directory Information Shadowing Protocol Edition: 1 (1998) withdrawn 2003

Reference in ICAO Document	Title and Current Status
ISO/IEC 9594:1995	(Generic reference to multi-part standard)
ISO/IEC 9594-1:1995	Information technology -- Open Systems Interconnection -- The Directory: Overview of concepts, models and services Edition: 4 (2001), Edition 5 (2005) [1990 ed 1 withdrawn in 1998; 1995 ed 2 withdrawn in 2000, 1998 ed 3 withdrawn in 2007]
ISO/IEC 9594-2	Information technology -- Open Systems Interconnection -- The Directory: Models Edition: 4 (2001), Edition 5 (2005) [1990 ed 1 withdrawn in 1998; 1995 ed 2 withdrawn in 2000, 1998 ed 3 withdrawn in 2007]
ISO/IEC 9594-5 : 1995	Information technology -- Open Systems Interconnection -- The Directory: Protocol specifications Edition: 4 (2001), Edition 5 (2005) [1990 ed 1 withdrawn in 1998; 1995 ed 2 withdrawn in 2000, 1998 ed 3 withdrawn in 2007]
ISO/IEC 9594-6:1995	Information technology -- Open Systems Interconnection -- The Directory: Selected attribute types Edition: 4 (2001), Edition 5 (2005) [1990 ed 1 withdrawn in 1998; 1995 ed 2 withdrawn in 2000, 1998 ed 3 withdrawn in 2007]
ISO/IEC 9594-7:1995 ISO/IEC 9594-7:1998.	Information technology -- Open Systems Interconnection -- The Directory: Selected object classes Edition: 4 (2001), Edition 5 (2005) [1990 ed 1 withdrawn in 1998; 1995 ed 2 withdrawn in 2000, 1998 ed 3 withdrawn in 2007]
ISO/IEC 9594-8 / X.509,	Information technology -- Open Systems Interconnection -- The Directory: Public-key and attribute certificate frameworks Edition: 4 (2001), Edition 5 (2005) [1990 ed 1 withdrawn in 1998; 1995 ed 2 withdrawn in 2000, 1998 ed 3 withdrawn in 2007]
(ISO/IEC 9646-1)	ISO/IEC 9646-1:1994 Information technology -- Open Systems Interconnection -- Conformance testing methodology and framework -- Part 1: General concepts Edition: 2 (1994)
ISO/IEC 9646-7	ISO/IEC 9646-7:1995 Information technology -- Open Systems Interconnection -- Conformance testing methodology and framework -- Part 7: Implementation Conformance Statements Edition: 1 (1995)
(ISO/IEC 9646-7:1995/Cor 1:1997)	Edition 1 (1997)
ISO/IEC 10181-1	ISO/IEC 10181-1:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Overview Edition: 1 (1996)
ISO/IEC 10181-2	ISO/IEC 10181-2:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Authentication framework Edition: 1 (1996)
ISO/IEC 10181-3	ISO/IEC 10181-3:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Access control framework Edition: 1 (1996)
ISO/IEC 10181-6	ISO/IEC 10181-6:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Integrity framework Edition: 1 (1996)

Reference in ICAO Document	Title and Current Status
ISO/IEC 11586-1	ISO/IEC 11586-1:1996 Information technology -- Open Systems Interconnection -- Generic upper layers security: Overview, models and notation Edition: 1 (1996)
ISO/IEC ISP 10611-1:1994.	Information technology -- International Standardized Profiles AMH1n -- Message Handling Systems -- Common Messaging -- Part 1: MHS Service Support Edition: 3 (2003) 1994 Ed 1 withdrawn 1997; 1997 Ed 2 withdrawn 2003
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 Edition: 2 (1994) 1994 Ed 1 withdrawn 1997
ISO/IEC ISP 10611-3:1994 (or a later edition),	Information technology -- International Standardized Profiles AMH1n -- Message Handling Systems -- Common Messaging -- Part 3: AMH11 -- Message Transfer (P1) Edition: 3 (2003) 1994 Ed 1 withdrawn 1997; 1997 Ed 2 withdrawn 2003
ISO/IEC ISP 10611-4:1994 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 (2003) 1994 Ed 1 withdrawn 1997; 1997 Ed 2 withdrawn 2003
ISO/IEC ISP 10611-5:1994 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 (2003) 1994 Ed 1 withdrawn 1997; 1997 Ed 2 withdrawn 2003
ISO/IEC ISP 10611-6:2003	Information technology -- International Standardized Profiles AMH1n -- Message Handling Systems -- Common Messaging -- Part 6: AMH15 - MS 94 Access (P7) Edition: 2 1998 Ed 1 withdrawn 2003
ISO/IEC ISP 10616-1	Information technology -- International Standardized Profile FD111 -- Directory data definitions -- Common Directory Use (Normal) Edition: 1 (1995)
ISO/IEC ISP 11188-1:1995.	ISO/IEC ISP 11188-1:1995 Information technology -- International Standardized Profile -- Common upper layer requirements -- Part 1: Basic connection oriented requirements Edition: 1 (1995)
ISO/IEC ISP 11189	Information technology -- International Standardized Profile FD12 -- Directory Data Definitions -- MHS Use of the Directory Edition: 1 (1997) – withdrawn in 2007. No current edition.
ISO/IEC ISP 11189 Amd 1	(Not in ISO catalogue)
ISO/IEC ISP 12062-1:1995 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 (2003) 1995 Ed 1 withdrawn 1998; 1998 Ed 2 withdrawn 2003
ISO/IEC ISP 12062-2:1995 ISO/IEC ISP 12062-2:2003	Information technology -- International Standardized Profiles AMH2n -- Message Handling Systems -- Interpersonal Messaging -- Part 2: AMH21 -- IPM Content Edition: 3 (2003) 1995 Ed 1 withdrawn 1997; 1997 Ed 2 withdrawn 2003

Reference in ICAO Document	Title and Current Status
ISO/IEC ISP 12062-3:1995 (or a later edition) 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 (2003) 1995 Ed 1 withdrawn 1997; 1997 Ed 2 withdrawn 2003
ISO/IEC ISP 12062-4:1995 (or a later edition) 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 (2003) 1995 Ed 1 withdrawn 1997; 1997 Ed 2 withdrawn 2003
ISO/IEC ISP 12062-5:1995 (or a later edition) 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 (2003) 1995 Ed 1 withdrawn 1997; 1997 Ed 2 withdrawn 2003
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: 1 (2003)
ISO/IEC ISP 15126-1	Information technology - International Standardised Profiles FDY1n – Directory data definitions – Part 1: FDY11 – Common directory use (normal) Edition: 1 (1999)
ISO/IEC ISP 15126-2	Information technology -- International Standardized Profiles FDY1n -- Directory data definitions -- Part 2: FDY12 -- Directory system schema Edition: 1 (1999)
ISO/IEC TR 10000-1:1995	ISO/IEC TR 10000-1:1998 Information technology -- Framework and taxonomy of International Standardized Profiles -- Part 1: General principles and documentation framework Edition: 4 (1998) 1995 Ed 3 withdrawn 1998
ISO/IEC TR 10000-2:1995	ISO/IEC TR 10000-2:1998 Information technology -- Framework and taxonomy of International Standardized Profiles -- Part 2: Principles and Taxonomy for OSI Profiles Edition: 5 (1998) 1995 Ed 4 withdrawn 1998
(ISO/IEC TR 10021-11:1999)	Information technology -- Message Handling Systems (MHS): MHS Routing -- Guide for messaging systems managers Edition: 1 (1999)
(ISO/IEC TR 18016:2003)	Information technology -- Message Handling Systems (MHS): Interworking with Internet e-mail Edition: 1 (2003)
CCITT Rec X.400 (1992)	ITU-T Recommendation F.400/X.400 (06/99): Message handling services: Message handling system and service overview (1992 and 1995 versions are Superseded)
CCITT Rec X.402 (1992)	ITU-T Recommendation X.402 (06/99): Information technology - Message Handling Systems (MHS): Overall architecture (1992 and 1995 versions are Superseded)
CCITT Rec X.411 (1992)	ITU-T Recommendation X.411 (06/99): Information technology - Message Handling Systems (MHS): Message Transfer System: Abstract Service Definition and Procedures (1992 and 1995 versions are Superseded)
CCITT Rec X.419 (1992)	ITU-T Recommendation X.419 (06/99): Information technology - Message Handling Systems (MHS): Protocol Specifications (1992 and 1995 versions are Superseded)

Reference in ICAO Document	Title and Current Status
CCITT Rec X.420 (1992)	ITU-T Recommendation X.420 (06/99): Information technology - Message Handling Systems (MHS): Interpersonal Messaging System (1992 and 1996 versions are Superseded)
CCITT Rec. X.217	ITU-T Recommendation X.217 (04/95): Information technology - Open Systems Interconnection - Service definition for the Association Control Service Element (Amendments 1 (1996) and 2 (1997) are In Force. 1992 version is Superseded)
ITU-T Rec. X.216	ITU-T Recommendation X.216 (07/94): Information technology - Open Systems Interconnection - Presentation service definition (Amendments 1 (1997) and 2 (1997) are In Force. 1995 version is Superseded)
ITU-T Rec. X.218	ITU-T Recommendation X.218 (03/93): Reliable Transfer: Model and service definition
ITU-T X.500:1993	ITU-T Recommendation X.500 (08/05): Information technology - Open Systems Interconnection - The Directory: Overview of concepts, models and services (02/01 and 08/05 versions are In Force, 1993 and 1997 versions are Superseded)
ITU-T Rec. X.519:1993	ITU-T Recommendation X.519 (08/05): Information technology - Open Systems Interconnection - The Directory: Protocol specifications (02/01 and 08/05 versions are In Force, 1993 and 1997 versions are Superseded)
ITU-T Rec. X.583	ITU-T Recommendation X.583 : Information technology - Open Systems Interconnection - The Directory: Protocol Implementation Conformance Statement (PICS) proforma for the Directory Access Protocol WITHDRAWN as irrelevant on 2006-02-09, as based on 1993 edition of X.500-series Recommendations
ITU-T Rec. X.584	ITU-T Recommendation X.584 : Information technology - Open Systems Interconnection - The Directory: Protocol Implementation Conformance Statement (PICS) proforma for the Directory System Protocol WITHDRAWN as irrelevant on 2006-02-09, as based on 1993 edition of X.500-series Recommendations
ITU-T Rec. X.881	ITU-T Recommendation X.881 (07/94): Information technology - Remote Operations: OSI realizations - Remote Operations Service Element (ROSE) service definition
RFC 0791:1981	(Also STD0005) Internet Protocol. J. Postel. September 1981. (Obsoletes RFC0760) (Updated by RFC1349) Status: STANDARD
RFC 0793:1981	(Also STD0007) Transmission Control Protocol. J. Postel. September 1981. (Updated by RFC3168) Status: STANDARD
RFC 1006:1987	(Also STD0035) ISO Transport Service on top of the TCP Version: 3. M.T. Rose, D.E. Cass. May 1987. (Obsoletes RFC0983) (Updated by RFC2126) Status: STANDARD
RFC 1122:1989	(Also STD0003) Requirements for Internet Hosts - Communication Layers. R. Braden, Ed. October 1989. (Updated by RFC1349, RFC4379) Status: STANDARD
RFC 2126:1997	ISO Transport Service on top of TCP (ITOT). Y. Pouffary, A. Young. March 1997. (Updates RFC1006) Status: PROPOSED STANDARD

Reference in ICAO Document	Title and Current Status
RFC 2401:1998	Security Architecture for the Internet Protocol. S. Kent, R. Atkinson. November 1998. (Obsoletes RFC1825) (Obsoleted by RFC4301) (Updated by RFC3168) Status: PROPOSED STANDARD
RFC 2460:1998	Internet Protocol, Version 6 (IPv6) Specification. S. Deering, R. Hinden. December 1998 (Obsoletes RFC1883) (Updated by RFC5095) Status: DRAFT STANDARD
RFC 2463:1998	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification. A. Conta, S. Deering. December 1998. (Obsoletes RFC1885) (Obsoleted by RFC4443) Status: DRAFT STANDARD
RFC 2488:1999	(Also BCP0028) Enhancing TCP Over Satellite Channels using Standard Mechanisms. M. Allman, D. Glover, L. Sanchez. January 1999. Status: BEST CURRENT PRACTICE
RFC 2560:1999	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams. June 1999 Status: PROPOSED STANDARD
RFC 2789:2000	Mail Monitoring MIB. N. Freed, S. Kille. March 2000 Obsoletes RFC2249, RFC1566) Status: PROPOSED STANDARD
RFC 2849:2000	The LDAP Data Interchange Format (LDIF) – Technical Specification. G. Good. June 2000 (Status: PROPOSED STANDARD
RFC 3411:2002	(Also STD0062) An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks. D. Harrington, R. Presuhn, B. Wijnen. December 2002 (Obsoletes RFC2571) (Updated by RFC5343, RFC5590) Status: STANDARD
RFC 3647:2003	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. S. Chokhani, W. Ford, R. Sabett, C. Merrill, S. Wu. November 2003 (Obsoletes RFC2527) Status: INFORMATIONAL
RFC 4510:2006	Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map. K. Zeilenga, Ed.. June 2006 (Obsoletes RFC2251, RFC2252, RFC2253, RFC2254, RFC2255, RFC2256, RFC2829, RFC2830, RFC3377, RFC3771) Status: PROPOSED STANDARD

A2.2.4 ICAO Doc 9880 Part IVA specifies that the directory aspects of ATN are based on the ISO/IEC standards identified in the following table. These standards have (almost) equivalent ITU-T Recommendations as identified in the second column of the table and these are taken into account in this EUROCONTROL Specification.

ISO/IEC Standard	Equivalent ITU-T Recommendation	Title
ISO/IEC 9594-1, 2001	X.500	The Directory: Overview of concepts, models and services
ISO/IEC 9594-2, 2001	X.501	The Directory: Models,
ISO/IEC 9594-8, 2001	X.509	The Directory: Authentication framework,
ISO/IEC 9594-3, 2001	X.511	The Directory: Abstract service definition,
ISO/IEC 9594-4, 2001	X.518	The Directory: Procedures for distributed operation,
ISO/IEC 9594-5, 2001	X.519	The Directory: Protocol specifications,
ISO/IEC 9594-7, 2001	X.521	The Directory: Selected object classes,



ISO/IEC Standard	Equivalent ITU-T Recommendation	Title
ISO/IEC 9594-9, 2001	X.525	The Directory: Replication,

A2.2.5 ICAO Doc 9705 Sub-Volume VIII specifies that the security aspects of ATN are based on the ISO/IEC standards identified in the following table. These standards have equivalent ITU-T Recommendations as identified in the second column of the table and these are taken into account in this EUROCONTROL Specification.

ISO/IEC Standard	Equivalent ITU-T Recommendation	Title
ISO/IEC 10181-1	X.810	Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Overview
ISO/IEC 10181-2	X.811	Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Authentication
ISO/IEC 10181-3	X.812	Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Access control framework
ISO/IEC 10181-6	X.815	Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Integrity framework
ISO/IEC 11586-1	X.830	Information technology -- Open Systems Interconnection -- Generic upper layers security: Overview, models and notation
ISO/IEC 10021	X.400 Series	Information technology -- Message Handling Systems (MHS)