

European Directory Service - WP4

EDS User Interface Manual

| | | |
|-----------------------|---|-----------------------|
| Edition Number | : | Version 1.0 |
| Edition Date | : | 04/09/2013 |
| Status | : | Released Issue |
| Intended for | : | AFSG |

DOCUMENT CHARACTERISTICS

| TITLE | | |
|--|------------------------|---------------------|
| <h3 style="margin: 0;">European Directory Service - WP4</h3> <h3 style="margin: 0;">EDS User Interface Manual</h3> | | |
| EATMP Infocentre Reference: | | |
| Document Identifier | Edition Number: | Version 1.0 |
| EDS/04 | Edition Date: | 04/09/2013 |
| Abstract | | |
| <p>The European Directory Service (EDS) Operational Concept is the result of the EUROCONTROL study on ATN Directory services in Europe. The EUR ICAO AFSG adopted the EDS Operational Concept as an appendix to the EUR AMHS Manual and invited States and Organisations to actively support implementation and validation of the EDS by EUROCONTROL.</p> <p>This work is related to activities at EUROCONTROL for implementation, validation and operation of the Central European DSA according to the first step of the EDS Operational Concept.</p> <p>This document is the EDS User Interface Manual, giving a brief summary of details for Co-operate and Adjacent Operators as well as engineering and maintenance personnel in order support these users in setup of communications, operation and trouble shooting.</p> | | |
| Keywords | | |
| EDS | Directory | User Interface AMHS |
| Contact Person(s) | Tel | Unit |
| | | |

| STATUS, AUDIENCE AND ACCESSIBILITY | | |
|--|---|--|
| Status | Intended for | Accessible via |
| Working Draft <input type="checkbox"/> | General Public <input type="checkbox"/> | Intranet <input type="checkbox"/> |
| Draft <input type="checkbox"/> | EATMP Stakeholders <input type="checkbox"/> | Extranet <input type="checkbox"/> |
| Proposed Issue <input type="checkbox"/> | Restricted Audience <input checked="" type="checkbox"/> | Internet (www.eurocontrol.int) <input type="checkbox"/> |
| Released Issue <input checked="" type="checkbox"/> | <i>Printed & electronic copies of the document can be obtained from the EATMP Infocentre (see page iii)</i> | |

| ELECTRONIC SOURCE | | |
|-------------------|-------------------------------|---------|
| Path: | EDS_User_Interface_Manual.doc | |
| Host System | Software | Size |
| Windows7 | Microsoft Word 14.0 | 2674 Kb |

EATMP Infocentre
EUROCONTROL Headquarters
96 Rue de la Fusée
B-1130 BRUSSELS

Tel: +32 (0)2 729 51 51

Fax: +32 (0)2 729 99 84

E-mail: eatmp.infocentre@eurocontrol.int

Open on 08:00 - 15:00 UTC from Monday to Thursday, incl.

DOCUMENT APPROVAL

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

| AUTHORITY | NAME AND SIGNATURE | DATE |
|--|--------------------|------------|
| <i>Please make sure that the EATMP Infocentre Reference is present on page ii.</i> | | |
| Project Manager | Yuksel Eyuboglu | 20/09/2013 |
| | | |
| | | |
| | | |
| | | |

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 | 28/06/2013 | | Initial draft version | All |
| 0.9 | 02/08/2013 | | Proposed issue after reviews | All |
| 1.0 | 04/09/2013 | | Released issue after final enhancements | 2, 2.2, 3.2, 5.1, 5.2, 7.2.3 |

CONTENTS

| | |
|---|-----------|
| 1. Introduction | 1 |
| 1.1 Scope of the Document..... | 1 |
| 1.2 Goal of the Document | 1 |
| 1.3 References..... | 2 |
| 1.4 Structure of the Document | 3 |
| 2. Overview | 4 |
| 2.1 Topology | 4 |
| 2.2 Flow of Information – Initial Step..... | 5 |
| 2.3 User Interface..... | 6 |
| 3. Interface Protocols..... | 8 |
| 3.1 Directory Information Shadowing Protocol..... | 8 |
| 3.2 Directory System Protocol..... | 8 |
| 4. Initial Contents | 10 |
| 4.1 AMHS MD Registry | 12 |
| 4.2 CAAS Mapping Information | 13 |
| 4.3 AMHS User Addresses and Capabilities | 13 |
| 5. Setup of Systems | 15 |
| 5.1 Prerequisites | 15 |
| 5.2 Peers..... | 17 |
| 5.3 Users..... | 20 |
| 6. Use of Information..... | 22 |
| 6.1 AFTN/AMHS Gateway | 22 |
| 6.2 ATS Message User Agent..... | 23 |
| 7. Trouble Shooting | 26 |
| 7.1 Sources of Malfunction..... | 26 |
| 7.2 Analysis..... | 26 |

List of Tables

| | |
|---|----|
| Table 1: Basic VPN Parameters | 17 |
| Table 2: Peer Parameters | 18 |
| Table 3: Shadowing Parameters | 19 |
| Table 4: Knowledge Reference Parameters | 20 |
| Table 5: User Parameters | 20 |
| Table 6: User Capabilities | 24 |
| Table 7: Object Identifier Values..... | 24 |

List of Figures

| | |
|---|----|
| Figure 1: EDS Topology | 5 |
| Figure 2: Unidirectional Flow of Information..... | 6 |
| Figure 3: EDS User Interface..... | 7 |
| Figure 4: EDS Base Entry and Managed Areas..... | 11 |
| Figure 5: EDS Target Structure of Managed Areas | 12 |

1. Introduction

The European Directory Service (EDS) is the implementation of ATN Directory services [5] in Europe. The EDS provides future, directory-based means for collection and distribution of information within Europe and exchange of information with other Regions, States and Organisations.

EUROCONTROL implements the Central European DSA for the initial step according to the EDS Operational Concept initially defined in the EUROCONTROL EDS Operational Concept document [12], adopted by the Aeronautical Fixed Services Group (AFSG) and published in the Appendix G to ICAO EUR Doc 020 (EUR AMHS Manual) [2].

In the initial step of the EDS Operational Concept the ATS Messaging Management Centre (AMC) is the single source of information for distribution by EDS. In support of the ATS Message Handling Service (ATSMHS) the AMC supplies related information to the Central European DSA which in turn distributes the information to Cooperating and Adjacent DSAs.

1.1 Scope of the Document

This document describes the user interface of EDS for Co-operating and Adjacent Operators and provides additional guidance material. It summarises interface details for the exchange of information between the Central European DSA, and Co-operating and Adjacent DSAs. The operators, engineering and maintenance personnel of Co-operating and Adjacent DSAs are the intended, primary audience of this document. In addition, this document might serve others as guidance material.

The EDS User Interface Manual recaps the protocols used between the involved entities, initial contents of EDS, and provides general details on the setup of communications. The manual also includes guidance material on the use of information in support of the AMHS and advice for trouble shooting.

The document represents the deliverable WP4.DEL1 of the EDS implementation at EUROCONTROL.

1.2 Goal of the Document

The purpose of this document is the establishment of an Interface Control Document (ICD) for the interface between the Central European DSA on the one hand and Co-operating and Adjacent DSA on the other hand. Furthermore it is the intention to deliver advice on the use of information and on trouble shooting.

The document summarises the communications means and the initial contents of EDS. It shall assist in setting up communications with the Central European

DSA and provide additional material on the use of information assist in trouble shooting.

Reader of this document should be familiar with the EDS Operational Concept specified in the Appendix G to the ICAO EUR Doc 020 (EUR AMHS Manual) [2].

1.3 References

The document makes reference to a number of international documents established and maintained by ICAO and EUROCONTROL. In turn, these documents also refer to ISO/IEC, ITU-T and IETF standards. In addition, the document makes direct use of small number of IETF standards.

- [1] EUROCONTROL-SPEC-0136 EUROCONTROL Specification on the Air Traffic Services Message Handling System (AMHS), Edition 2.0, 18/09/2009

Note: Specification's reference published as a Community specification in the Official Journal of the European Union, C 323/24, 31.12.2009.

- [2] ICAO EUR Doc 020 EUR AMHS Manual, Version 8.0, 25/04/2013
- [3] ICAO EUR Doc 021 ATS Messaging Management Manual, Version 9.0, 25/04/2013
- [4] ICAO Doc 9880 AN/466 Manual on Detailed Technical Specifications for the Aeronautical Telecommunication Network (ATN) using ISO/OSI Standards and Protocols, Part II — Ground-Ground Applications — Air Traffic Services Message Handling Services (ATSMHS), 1st Edition, 2010
- [5] ICAO Doc 9880 AN/466 Manual on Detailed Technical Specifications for the Aeronautical Telecommunication Network (ATN) using ISO/OSI Standards and Protocols, Part IV — Directory Services, Security and Systems Management, 1st Edition, 2010
- [6] ICAO Doc 9896 Manual on the Aeronautical Telecommunication Network (ATN) using Internet Protocol Suite (IPS) Standards and Protocols, 1st Edition, 2010
- [7] ISO/IEC 7498-1 Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model, 2nd Edition, 1994
- [8] ISO/IEC 9594-n Information technology – Open Systems Interconnection – The Directory (multi-part), 5th Edition, 2005

Note: This set of standards was also published as ITU-T X.500 (08/2005) set of standards.

- [9] ISO/IEC 10021-7 Information technology – Message Handling Systems (MHS) – Interpersonal Messaging System, 2003
- [10] IETF RFC 1006 ISO Transport Service on top of the TCP, Version: 3, May 1987
- [11] IETF RFC 2126 ISO Transport Service on top of TCP (ITOT), March 1997
- [12] EUROCONTROL European Directory Service (EDS) – Operational Concept – WP2 (Concept), Version 1.0, 26/10/2011

1.4 Structure of the Document

This document composes of the following chapters:

- Chapter 1 (this chapter) contains an introduction to the document.
- Chapter 2 gives an overview on EDS and the User Interface.
- Chapter 3 specifies the interface protocols.
- Chapter 4 describes details of the initial contents.
- Chapter 5 provides guidance on setup of systems
- Chapter 6 outlines use of information in support of the AMHS
- Chapter 7 gives assistance for trouble-shooting.

2. Overview

This chapter summarises the basic elements of the EDS Operational Concept and provides a brief introduction to the EDS user interface.

The EDS Operational Concept adopts and refines the approach given by the AMHS Community Specification [1], further referred to as AMHS CS. In chapter 4, the AMHS CS outlines a central Directory service as a European Common Facility.

In addition to an isolated European solution, the EDS Operational Concept considers the global aspect of Directory services. Regions, States, and Organisations not directly participating in the concept, need to exchange data with the central DSA and/or States and Organisations participating in the concept. Regions, States and Organisation not participating in the concept also provide data that is required by the participating States and Organisations as well as vice versa.

The EDS Operational Concept given in the Appendix G to ICAO EUR Doc 020 (EUR AMHS Manual) [2] considers existing implementations, current network infrastructure, established management procedures and proposes a three-step transition process consisting of the initial, intermediate and final step. This document focuses on the initial step of the EDS Operational Concept.

2.1 Topology

The EDS Operational Concept describes an overall online Directory solution. In the framework of the European Directory Service the term “online” refers to a service that provides direct and automated communication means between the involved entities using well-defined protocols. Communication is established and usually takes place on demand or by schedule. Manual initiation or intervention by human users on a regular basis is not foreseen. A permanent exchange of information on a 24 hour basis is not implied by the term online.

The EDS Operational Concept as specified in the Appendix G to ICAO EUR Doc 020 (EUR AMHS Manual) [2] specifies the relationship of the Central European DSA with Co-operating and Adjacent DSAs in participating and non-participating States and Organisations. Figure 1 gives an abstract overview of the EDS topology.

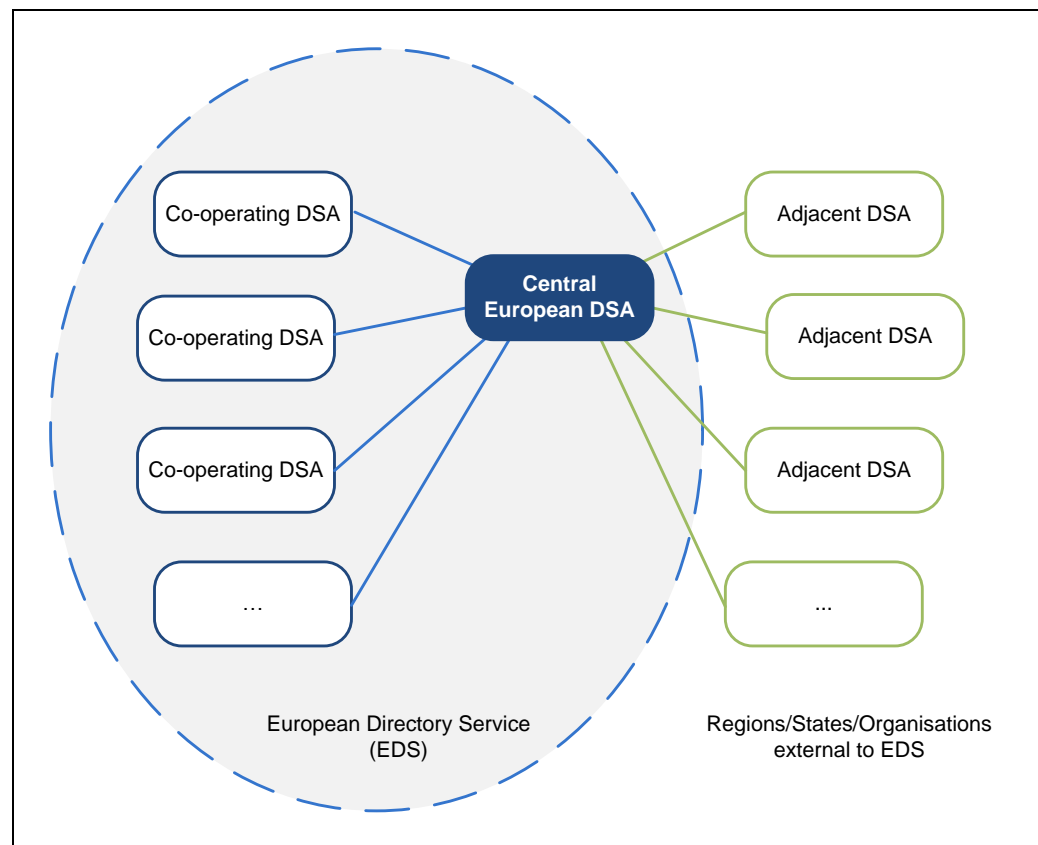


Figure 1: EDS Topology

These States and Organisations forming Directory Management Domains (DMDs) may implement further, subordinate DSAs in support of geographical deployment, quality of service, high availability, etc. Those subordinate DSAs may communicate among themselves and with the DMD's top level DSA; however they do not communicate with the central DSA and do not directly participate in the concept. Subordinate DSAs implemented by DMDs are therefore considered out of scope in the context of the EDS Operational Concept.

2.2 Flow of Information – Initial Step

In the initial step of EDS, the ATS Messaging Management Centre (AMC) remains the single source of relevant information. CCC Operators and AMC Operators remain in charge of management, consolidation and distribution of information. The EDS complements the AMC services and serves as a second means for distribution of information.

In line with the procedures specified in ICAO EUR Doc 021 (ATS Messaging Management Manual) [3], the AMC periodically provides relevant information to the Central European DSA, which in turn distributes the modifications to Co-operating and Adjacent DSAs of States and Organisations. These periodical events are

- Pre-operational Area achieves the status released; and
- Pre-operational Area with status released is moved to the Operational Area

Overall it can be stated, that there is a unidirectional flow of information in the initial step of EDS. The basic flow of information in the initial step of the EDS Operational Concept as specified by the EUR AMHS Manual [2] is outlined in Figure 2 below.

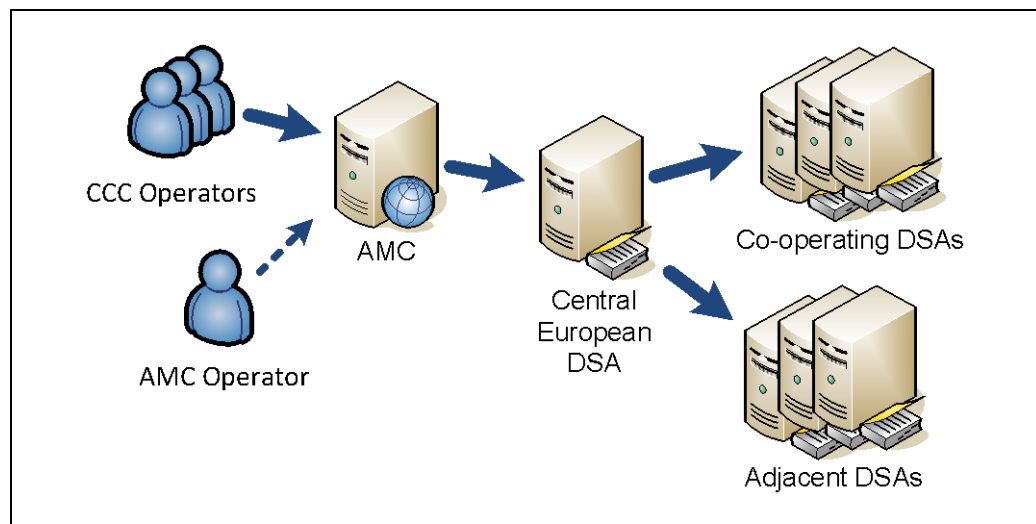


Figure 2: Unidirectional Flow of Information

The processing of the information provided by the Central European DSA and provision of information to end users is a local matter and considered out of scope.

2.3 User Interface

The focus of this document is the user interface of EDS as outlined in Figure 3. In this context, EDS users are identified as the users of the central service provided by the Central European DSA as a common facility. In other words, this document is concerned with aspects of the interface between the Central European DSA and the Co-operating and Adjacent DSAs only.

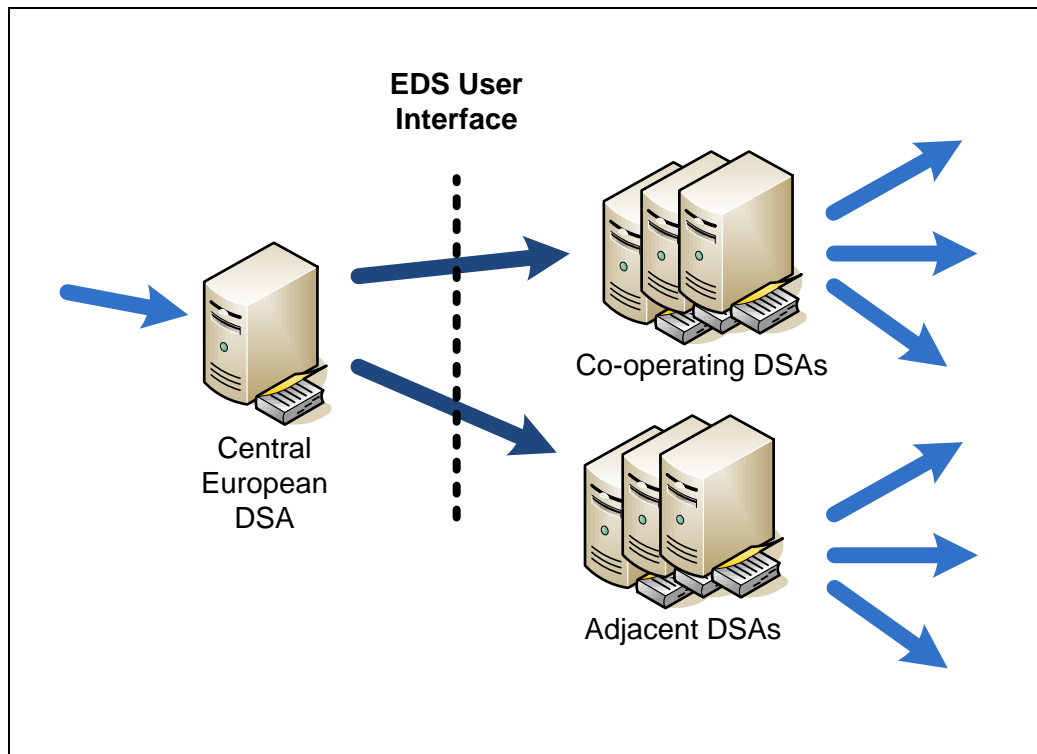


Figure 3: EDS User Interface

ICAO EUR Doc 020 (EUR AMHS Manual) [2] specifies in Appendix G the EDS Operational Concept. The EDS Operational Concept also addresses this interface.

3. Interface Protocols

This chapter recaps the X.500 protocols used between peer DSAs.

The EDS Operational Concept identifies two X.500 standards protocols for exchange of information between the Central European DSA, and Co-operative and Adjacent DSAs.

3.1 Directory Information Shadowing Protocol

The Directory Information Shadowing Protocol (DISP) specified in ISO/IEC 9594-9 [7] supports shadowing between two DSAs where a copy of a sub-tree of the Directory Information Tree (DIT) is made available at another DSA. Shadowing is the standard way of replication for X.500-based Directory services. Following the proposal introduced by the AMHS CS [1], the EDS Operational Concept recommends DISP for the purpose of distribution of information from the Central European DSA to Co-operating and Adjacent DSAs.

Before shadowing can occur between a pair of DSAs, a shadowing agreement needs to be established between the involved parties. A shadowing agreement defines a unique identifier and version, as well as other parameters such as the unit of replication and the update mode.

When DISP is used for distribution of information within EDS, the Central European DSA always acts as the supplier of the information and the Co-operative or Adjacent DSA always takes the role of the consumer of the information. On change of information the Central European DSA initiates shadowing providing an incremental update of the information that has changed. In order to perform shadowing the Central European DSA invokes the shadowing operations. Prior to perform shadowing, the Central European DSA establishes an application association as necessary using the operation *DSA Shadow Bind*. Shadowing is performed by the operations *coordinateShadowUpdate* and *updateShadow*.

3.2 Directory System Protocol

The Directory System Protocol (DSP) specified in ISO/IEC 9594-5 [7] supports communications between two DSAs, where a request for information cannot be fully resolved by one DSA and is forwarded to another DSA.

Taking into account available products, implementations and the fact, that DISP was not mandated by ICAO Doc 9880 Part IV [5] or the AMHS CS [1], the EDS Operational Concept allows for other, non-standard or proprietary means of bulk retrieval from the Central European DSA using chaining by DSP.

When DSP is used to retrieve information from the Central European DSA, the Co-operating or Adjacent DSA acts as the initiator of uni-chained interrogation operations such as *Chained Read* and *Chained List*. Bulk retrieval needs to be initiated by a specialised Directory User Agent (DUA) that indirectly initiates the chained operation by emitting interrogation operations to the local, Co-operating or Adjacent DSA. Prior to perform chained interrogation operations the Co-operating and Adjacent DSA establishes an application association.

Please note, whereas shadowing is the primary means for distribution of information within EDS (push distribution), States and Organisations might implement specialised DUAs in order to indirectly retrieve the information from the Central European DSA through their local Co-operating or Adjacent DSAs (pull distribution). It is not the intention to retrieve the information on a case by case basis, but to retrieve a full copy of relevant information using chained operations of DSP.

4. Initial Contents

This chapter identifies the contents initially available in the initial step of EDS.

The AMHS as specified in ICAO Doc 9880 Part II [4] is one of the target applications to be supported by the ATN Directory services. Currently, the ATS Messaging Management Centre (AMC) as specified in ICAO EUR Doc 021 (ATS Messaging Management Manual) [3] manages and holds a portion of the information that has been already planned for distribution by Directory services. The information is required for

- Address conversion in support of the AFTN/AMHS Gateway and
- Determination of AMHS user capabilities in support of the ATS Message User Agent and the AFTN/AMHS Gateway.

Enabling the exchange of ATS messages between the AFTN and the AMHS, the Message Control and Transfer Unit (MTCU) of the AFTN/AMHS Gateway is in charge of the conversion between AFTN and AMHS addresses, and vice versa.

Different capabilities are associated with AMHS users such as maximum length of message contents and support of different message content types. In order to make use of only supported elements and to avoid Non-delivery Reports (NDRs) in the AMHS, a message originator needs to determine the capabilities of the intended recipients prior to submit the AMHS message.

The specification of the ATN Directory as laid down in ICAO Doc 9880 Part IV [5] also covers address information required for AFTN/AMHS address conversion as well as the AMHS user capabilities.

It should be noted that on-going work of the AFSG regarding the revision of AMHS user capabilities is not yet considered by the EDS Operational Concept.

The EDS Operational Concept merges two approaches for management and distribution of relevant information. The specification of the ATN Directory as specified by ICAO Doc 9880 Part IV [5] describing an online service and the offline management of information as specified in ICAO EUR Doc 021 (ATS Messaging Management Manual) [3].

In the initial step of EDS, the AMC manages and provides the relevant information on a periodic basis to EDS. The AMC remains the single source of information. The Central European DSA in turn distributes this information by a second means. There is no modification of information within EDS in the initial step.

Within ATS Messaging Management, there are two areas for distribution of information: the Pre-operational and the Operational Area. EDS adopted these areas and allocated them as Managed Areas directly below the EDS base

entry which is allocated directly below the virtual root. The EDS base entry is of the object-class *organization*. The naming attribute of type *organizationName* takes the value "European-Directory". The managed areas are represented by entries of standard object class *organizationalUnit*. The naming attributes of type *organizationalUnitName* take the value of the respective managed area, i.e. the areas are identified as "Pre-operational" and "Operational". The attribute type *description* indicates the cycle of ATS Messaging Management through a string (e.g. OPER.132) and allows for distinction of information belonging to two different cycles.

The general target structure for EDS given in Figure 4 shows the allocation of the Managed Areas below the EDS base entry.

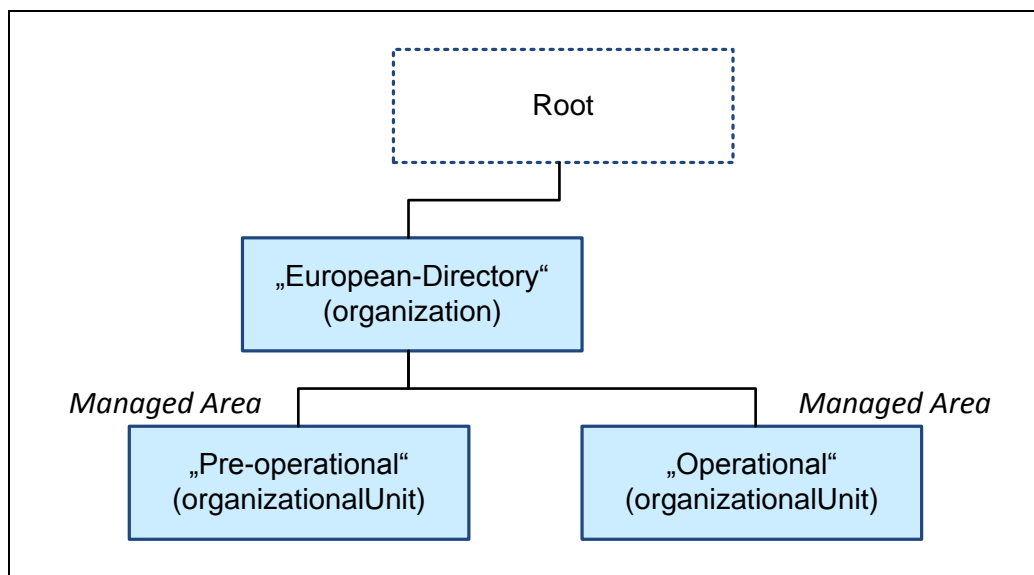


Figure 4: EDS Base Entry and Managed Areas

The pre-operational and operational areas are structured identically as outlined in Figure 5.

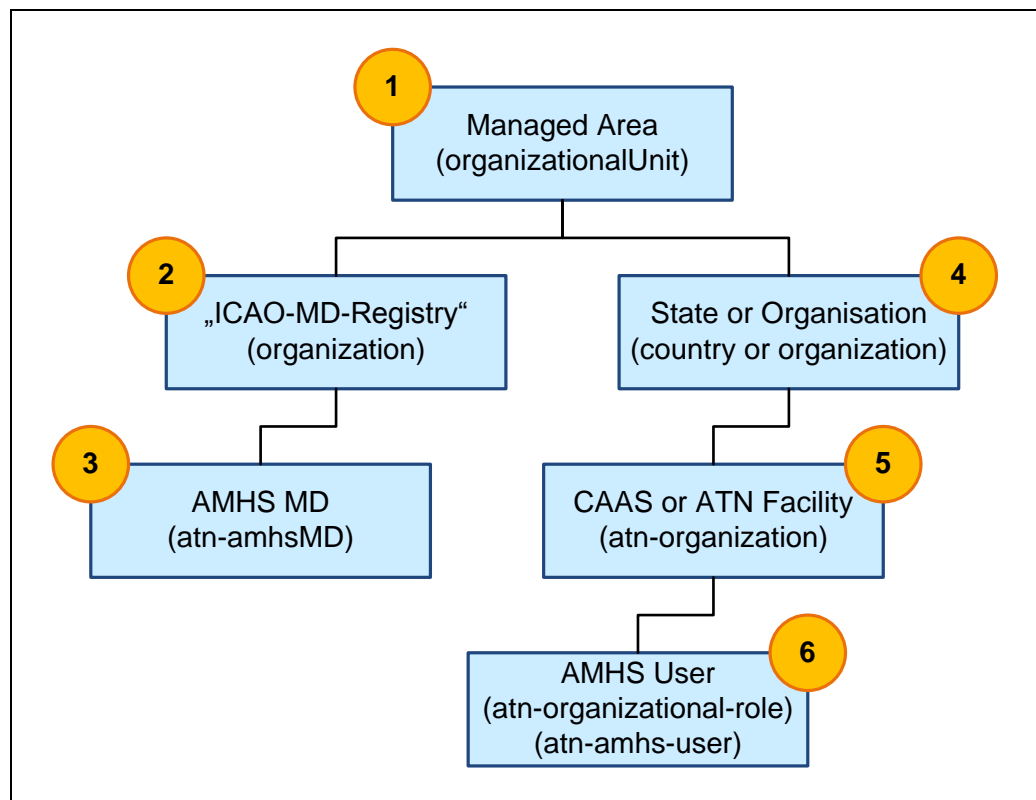


Figure 5: EDS Target Structure of Managed Areas

Figure 5 shows the allocation of the respective managed area (1), the ICAO MD Registry (2) including subordinate entries (3), the States and Organisations (4), CAAS mapping information resp. ATN facilities (5), and AMHS users (6).

Derived from the ICAO Doc 9880 Part IV [5], the target structure of EDS' managed areas as given in Figure 5 holds the following information:

- AMHS MD Registry;
- CAAS mapping information;
- AMHS user address information; and
- AMHS user capabilities.

4.1 AMHS MD Registry

The information of the ICAO Register of AMHS Management Domains (AMHS MD Registry) is maintained by AMC and originates from AMC's address management function.

The AMHS MD Registry is represented by a base entry of standard object class *organization* with the value of the naming attribute *organizationName* set to "ICAO-MD-Registry" and its subordinate entries.

The AMHS MD Registry includes at least one entry for each State or Organisation of atn-specific object class *atn-amhsMD* which is specified as follows:

```
atn-amhsMD OBJECT-CLASS ::= {
    SUBCLASS OF      { top }
    MUST CONTAIN     { common-name |
                    atn-global-domain-identifier |
                    atn-icao-designator,
                    atn-amhsMD-addressing-scheme }
    MAY CONTAIN      { atn-amhsMD-naming-context }
    ID               id-oc-atn-amhsMD }
```

Please refer to ICAO EUR Doc 020 (EUR AMHS Manual) [2], Appendix G for details on the specification of attribute types.

4.2 CAAS Mapping Information

The CAAS mapping information is maintained by AMC and originates from AMC's CAAS tables.

Each State is represented by an entry of standard object class *country* and each Organisation is represented by a standard object class *organization*.

Below the States' and Organisations' base entries, the CAAS mapping information is held using entries of atn-specific object class *atn-organization*. The object class *atn-organization* is derived from the standard object class *Organization* and is specified as follows:

```
atn-organization OBJECT-CLASS ::= {
    SUBCLASS OF      { Organization }
    MUST CONTAIN     { atn-facility-name }
    MAY CONTAIN      { atn-per-certificate |
                    atn-der-certificate }
    ID               id-oc-atn-Organization }
```

Please refer to ICAO EUR Doc 020 (EUR AMHS Manual) [2], Appendix G for details on the specification of attribute types.

4.3 AMHS User Addresses and Capabilities

An AMHS user is represented by an entry of atn-specific object class *atn-organizational-role* with an atn-specific, auxiliary object class *atn-amhs-user*. The object class *atn-organizational-role* is derived from the standard object class *organizationalRole*. The atn-specific object classes are specified as follows:

```
atn-organizational-role OBJECT-CLASS ::= {  
    SUBCLASS OF      { organizationalRole }  
    MUST CONTAIN     { }  
    MAY CONTAIN      { atn-per-certificate |  
                     atn-der-certificate }  
    ID               id-oc-atn-OrganizationalRole }
```

```
atn-amhs-user OBJECT-CLASS ::= {  
    SUBCLASS OF      { top }  
    KIND             AUXILIARY  
    MUST CONTAIN     { mhs-or-addresses |  
                     atn-ipm-heading-extensions |  
                     atn-amhs-direct-access }  
    MAY CONTAIN      { mhs-maximum-content-length |  
                     mhs-deliverable-content-types |  
                     mhs-acceptable-eits |  
                     mhs-exclusively-acceptable-eits |  
                     mhs-message-store-dn |  
                     atn-per-certificate |  
                     atn-der-certificate |  
                     atn-AF-address }  
    ID               id-oc-atn-AmhsUser }
```

Note: Auxiliary object classes such as the object class *atn-amhs-user* can be associated with structural object classes; however they are not suitable to structure the DIT.

Please refer to ICAO EUR Doc 020 (EUR AMHS Manual) [2], Appendix G for details on the specification of attribute types.

5. Setup of Systems

This chapter addresses general prerequisites and configuration of networks and implementations describing the parameters.

A basic prerequisite is a common underlying network infrastructure in order to establish communication between the peer DSAs. Minor prerequisites apply to the Co-operating and Adjacent DSAs.

The setup of communications requires a number of fixed parameters and some additional parameters to be agreed and exchanged.

5.1 Prerequisites

In the EDS, peer DSAs make use of the Directory Information Shadowing Protocol (DISP) or the Directory System Protocol (DSP) as already outlined in chapter 3. These protocols in turn are based on the 7-layer ISO Open Systems Interconnection (OSI) model as given in ISO/IEC 7498-1 [7]. Where DISP is not supported by an implementation, distribution of information could be achieved through DSP requiring some additional effort for implementation of a specialised DUA for implementation of pull distribution.

EDS follows the principles of IP-based networking set out in the ICAO Doc 9896 [6] and ICAO EUR Doc 020 (EUR AMHS Manual) [2]. At the transport layer, deviating from the ISO/OSI model, EDS peer communication deploys the Transmission Control Protocol (TCP) and the Internet Protocol version 4 (IPv4) by providing an ISO transport service on top of TCP according to RFC 1006 [9]. In support of future use of the Internet Protocol version 6 (IPv6), implementations should provide an ISO transport mapping on top of TCP according to RFC 2126 [11].

The use of TCP/IP enables the deployment of a wide range of commercial Directory products and use of existing, common network infrastructure.

Implementations intended for participation in the EDS as Co-operating DSA or to exchange information with EDS as Adjacent DSA shall implement a Directory System Agent in line with the X.500 base standards [8] and profiles identified by ICAO Doc 9880 Part IV [5] and the AMHS Community Specification [1]. Support of DISP is strongly recommended however not mandated. The implementation shall provide support for the ATN-specific attribute types and object classes, and shall implement the EDS Directory schema given in the appendix G to the ICAO EUR Doc 020 (EUR AMHS Manual) [2]. Implementations as a minimum should incorporate an Operational Personnel DUA as specified in ICAO Doc 990 Part IV.

In terms of the underlying network there are two options to establish communications with the Central European DSA.

It should be noted that communications between EDS peers occur in bursts during distribution of information.

Pan-European Network Service

The preferred option for the underlying network is the Pan-European Network Service (PENS). PENS is an international ground/ground communications infrastructure jointly implemented by EUROCONTROL and the European air navigation service providers (ANSPs) in order to meet existing and future air traffic communication requirements. PENS provides a common IP-based network service across the European region. EDS makes use of the following PENS VPNs:

- Test VPN for validation and test purposes
- Operational VPN for operation (proposed)

Virtual Private Network/Internet

A site to site Virtual Private Network (VPN) established over the public Internet is the secondary option which could be made available after mutual agreement. The establishment of a VPN is based Internet Protocol Security (IPSec) and requires the negotiation of additional, VPN-related parameters between the parties involved. Table 1 lists the basic parameters for VPN negotiations.

| Parameter | Central European DSA | Co-operating or Adjacent DSA |
|---|----------------------|------------------------------|
| Configuration Information | | |
| Tunnel End Point IP Address | | |
| Accessible Hosts/Networks | | |
| Network Address Translation | | |
| Service Ports | | |
| Phase 1: Internet Key Exchange Protocol (IKE) | | |
| Pre-shared Key | | |
| Authentication Algorithm | | |
| Encryption Algorithm | | |
| Diffie-Hellman Group | | |
| Negotiation Mode | | |
| Lifetime Measurement | | |
| Data | | |
| Time | | |

| Parameter | Central European DSA | Co-operating or Adjacent DSA |
|------------------------------|----------------------|------------------------------|
| Phase 2: IP Security (IPSec) | | |
| Authentication Algorithm | | |
| Encryption Algorithm | | |
| Encapsulation Mode | | |
| Diffie-Hellman Group (PFS) | | |
| Lifetime Measurement | | |
| Data | | |
| Time | | |

Table 1: Basic VPN Parameters

Support of VPN elements and features depends on the implementations of the respective routers. If supported, it is proposed to make use of the following VPN parameters:

- Authentication
 - Encapsulating Security Payload (ESP)
 - Secure Hash Algorithm 1 (SHA1)
 - Hash-based Message Authentication Code (HMAC) of 160 bit
- Advanced Encryption Standard (AES) with 256-bit
- Diffie Hellman Group 5 (1536 bits)
- Negotiation mode: Main
- Encapsulation mode: Tunnel
- Lifetime measurement based on time
 - 86400 seconds for IKE
 - 3600 seconds for IPSec

Secure communication means shall be used for the delivery of the pre-shared key.

For communications over the Internet (VPN) a bandwidth of 64 Kbit/s is proposed as a minimum.

5.2 Peers

Within EDS, identification of a DSA is achieved by its Distinguished Name (DN). EDS requires only simple authentication which implies the use of passwords. In other words, each communication peer is authenticated by its DN and password. The DNs and passwords form the credentials used in the

bind operations, DSA Bind in case of DSP and DSA Shadow Bind in case of DISP.

Furthermore a presentation address is associated with each DSA in order to address the application entity of the communication peer in the network. A presentation address is composed of the following:

- Presentation selector;
- Session selector;
- Transport selector; and
- Network address.

In the EDS it is proposed to omit presentation, session and transport selectors, i.e. the selectors are not present in the presentation address. The network address is composed of the IP address (e.g. 87.177.134.46) and the TCP port. Depending on network firewalls performing network address translation (NAT) the IP address needs to be adjusted accordingly. TCP port 102 is well known for ISO services on top of TCP, but other TCP ports may be used depending on local requirements.

Table 2 provides an overview on the parameters required to setup peers. This table could be used to bilaterally agree on and exchange the peer parameters.

| Parameter | Central European DSA | Co-operating or Adjacent DSA |
|-----------------------|-----------------------------|-------------------------------------|
| Distinguished Name | | |
| Password | | |
| Presentation Selector | | |
| Session Selector | | |
| Transport Selector | | |
| Network Address | | |

Table 2: Peer Parameters

The way and steps required to configure the peer parameters depend on the implementation.

Shadowing

Shadowing using DISP is the preferred option for distribution of information. EDS makes use of supplier initiated, incremental updates triggered automatically on change. Further details on shadowing using DISP are given in section 3.1.

The shadowing agreement established off-line between supplier and consumer defines:

- Agreement identifier: Unique identifier and version;
- Unit of replication; and
- Mode.

Table 3 provides an overview on the parameters required to setup a shadowing agreement. This table could be used to bilaterally agree on and exchange the shadowing parameters.

| Parameter | Central European DSA | Co-operating or Adjacent DSA |
|---------------------|----------------------------------|------------------------------|
| Identifier | See below | |
| Version | 0 (See also below) | |
| Role | Supplier | Consumer |
| Unit of replication | O=European-Directory | |
| Mode | Supplier Initiated, On Change | |
| Access Point | Central European DSA (See Peers) | |

Table 3: Shadowing Parameters

The parameter identifier of the agreement is required to be unique with regard to the pair of peer DSAs. The Central Administrator provides the value of the parameter identifier. The value of the parameter version is initially set to zero. In the unlikely case of a modification of the agreement, the involved parties might agree to increment the parameter version. In case of a modification of the agreement, the Central European DSA performs a total update.

The way and steps required to configure shadowing depend on the implementation.

Chaining

Chaining using DSP is a secondary means for distribution of information. The Co-operating or Adjacent DSA triggers this activity as given in section 3.2.

In order to setup chaining, the Co-operating or Adjacent DSA has to define a knowledge reference. A knowledge reference associates a distinguished name in the DIT including the sub-tree below with a DSA holding the entry.

In order to allow a Co-operating or Adjacent DSA to perform chained operations, a knowledge reference is required. The knowledge reference of type subordinate reference associates the entry with the distinguished name O=European-Directory with the Central European DSA.

Table 4 provides an overview on the parameters required to setup a knowledge reference.

| Parameter | Co-operating or Adjacent DSA |
|----------------|----------------------------------|
| Content Prefix | O=European-Directory |
| Type | Cross Reference |
| Access Point | Central European DSA (See Peers) |

Table 4: Knowledge Reference Parameters

The way and steps required to configure chaining depend on the implementation.

5.3 Users

While the EDS user interface describes the relation between Central European DSA and the Co-operating or Adjacent DSAs, this section addresses users of the EDS accessing the information stored within the EDS.

Within EDS, identification of users is achieved by Distinguished Names (DNs). EDS requires only simple authentication which implies the use of passwords. In other words, each user is authenticated by its DN and password. The DN and passwords form the credentials used in the *directoryBind* operation. Prior to perform any DAP operation, users have to authenticate against EDS using the *directoryBind* operation. Users always bind to their local Co-operating or Adjacent DSA.

Table 2 provides an overview on the parameters required to setup users. This table could be used to exchange user parameters.

| Parameter | User |
|--------------------|------|
| Distinguished Name | |
| Password | |

Table 5: User Parameters

EDS identifies to types of users:

- Operators of Co-operating and Adjacent DSAs; and
- End users.

Access to EDS by end users being either a human or system users is restricted to interrogation operations to the operational area with the distinguished name O=European-Directory; OU=Operational.

The way and steps required to configure end user is a local matter of Co-operating and Adjacent DSAs and depend on the implementation deployed as Co-operating or Adjacent DSA.

Co-operating and Adjacent Operators have to register with the Central European DSA, as – at a later stage – these users will have the right to

perform modification operations. After successful registration, the Central Administrator creates a user entry for the respective Co-operating and Adjacent Operator, and provides him with his password. Co-operating and Adjacent Operators may perform interrogation and modification operation on their own entry, allowing them to change their password.

Co-operating and Adjacent Operators can also perform interrogation operations on the pre-operational area. Access to the pre-operational area enables Co-operating and Adjacent Operators to prepare the information for legacy, not directory-aware implementations. Preparation of information is a local matter depending on the implementation of the legacy implementation.

Please note, in the intermediate and final step of EDS Co-operating Operators can perform modification operations to their data in the background area of EDS. The background area is not utilised in the initial step of EDS.

6. Use of Information

This chapter provides guidance on the use of information initially provided by EDS.

The EDS describes the information and the exchange of information between the Central European DSA, and Co-operating and Adjacent DSA. The further processing, the optional, local distribution and the use of information is considered out of scope of this document.

However, it is the intention of this chapter to provide users with guidance on the use of information provided by EDS.

6.1 AFTN/AMHS Gateway

The Message Transfer and Control Unit (MTCU) of the AFTN/AMHS Gateway is in need of address conversion between AMHS AF- and AMHS MF-addresses and determination of AMHS user capabilities.

ICAO Doc 9880 Part II [4] describes the conversion of addresses using tables. This section outlines one potential way for the conversion of addresses using the EDS following the principles given by ICAO Doc 9880 Part II. Please note, there might be other ways of achieving identical results.

AFTN to AMHS address conversion

The address conversion for AMHS AF- into AMHS MF-addresses comes in up to three steps which might also be used for the reverse address lookup on address conversion for AMHS MF- to AMHS AF-addresses:

- Check for individual information for this AMHS user.
- Determine the AMHS MD of this user, the associated Global Domain Identifier (GDI), addressing scheme and naming context.
- Determine the X.400 address attribute organization to complete the AMHS MF-address of the user.

First, search the EDS for an individual entry of object class *atn-amhs-user* with the attribute type *atn-AF-address* taking the value of the full AMHS AF-address. If an entry matches the criteria, terminate address conversion successfully, otherwise proceed.

Second, if no individual entry exists, the address conversion follows the algorithmic mapping of addresses. Starting with seven characters of the AMHS AF-address down to two (ICAO designators), search the ICAO MD Registry for an entry with a value of the attribute type *atn-icao-designator* matching the ICAO designators determined from the AMHS AF-address. If no matching entry could be determined, the address conversion terminates

unsuccessfully; otherwise store the value of the attribute type *atn-global-domain-identifier*. If the addressing scheme identified by the value of the attribute type *atn-amhsMD-addressing-scheme* corresponds to the XF addressing scheme, terminate the address conversion successfully; otherwise proceed.

Third, search within the State's or Organisation's entries indicated by the value of the attribute type *atn-amhsMD-naming-context* for the mapping of the location indicator onto the geographical unit. In order to meet the use of wildcards in CAAS mapping information, search the values of the attribute type *organizationName* of object class *organization* for the location indicator of the AMHS AF-address starting with all four down to one character. If a match could be determined, terminate the conversion successfully; otherwise terminate the search unsuccessfully.

In case of successful termination in the first step, determine the AMHS MF-address from the value of the attribute type *mhs-or-addresses*; otherwise determine the X.400 address attributes *country-name*, *administration-domain-name*, and *private-domain-name* from the stored GDI and complete AMHS MF-address depending on the addressing scheme as follows:

- XF addressing scheme: Set the X.400 address attribute *organization-name* to the fixed value "AFTN", and set the first element of the X.400 address attribute *organizational-unit-names* to the value of the AMHS AF-address.
- CAAS: Set the X.400 address attribute *organization-name* to the value determined by the EDS attribute type *atn-facility-name*, set the first element of the X.400 address attribute *organizational-unit-names* to the value of the 4-character location indicator of the AMHS AF-address, and set the X.400 address attribute *common-name* to the full, 8-character AMHS AF-address.

AMHS User Capability

In order to determine the appropriate format of the AMHS message, the MTCU needs to determine the AMHS user capability of the intended recipients. Please refer to section 6.2 for determination of user capabilities.

6.2 ATS Message User Agent

In support of the Extended ATS Message Handling Service an ATS Message User Agent needs to determine through its DUA the capabilities of the AMHS recipient(s) prior to encode the AMHS message. The capabilities are used to determine the level of support by the AMHS recipient(s) and to generate the AMHS message according to the common, minimum level of support.

Determination of AMHS User Capabilities

According to ICAO Doc 9880 Part II [4], an AMHS user supporting the Extended ATS Message Handling Service is identified by its AMHS MF-

address and additionally by its Directory name which is a distinguished name. However, in case the Directory name is not available, it could be determined by searching the EDS for a match of the recipient's AMHS MF-address.

In order to determine the capabilities of an AMHS user, a simple read operation using his Directory name is sufficient. In case the read operation reports success, the attribute types of object class *atn-amhs-user* deliver the user's capabilities; otherwise capabilities of the user are not available in EDS.

The individual capabilities of an AMHS user is determined from the attribute types as given in Table 6.

| Attribute Type | Description |
|---------------------------------|--|
| atn-ipm-heading-extensions | Support of AMHS Functional Group IHE. Value is true or false depending on support of Extended ATSMHS. |
| atn-amhs-direct-access | Direct or indirect AMHS user. Value is true or false depending on type of user. |
| mhs-maximum-content-length | Maximum deliverable content length. Value indicates the maximum number of octets. |
| mhs-acceptable-eits | Attribute type is for further study. |
| mhs-exclusively-acceptable-eits | Supported Encoded Information Types (EITs). Value specification may be repeated (multi-valued). Values are Object Identifiers (OIDs). See below for further details. |

Table 6: User Capabilities

The optional attribute type *mhs-exclusively-acceptable-eits* is a list of Object Identifiers (OIDs) representing the user's capabilities with regard to different types of information. Following OID values are used to indicate the user's support of content types.

| Capability | Object Identifier Values |
|-------------------------------|---|
| IA5 Text | 2.6.3.4.2 (ia5-text) |
| General Text | 1.0.10021.7.1.0.1 (basic control set C0), 1.0.10021.7.1.0.6 (graphics set G0 US ASCII), 1.0.10021.7.1.0.100 (graphics set G1 Basic-1) |
| Bilaterally Defined Body Part | 2.6.3.4.0 (undefined) |
| File Transfer Body Part | 2.6.1.12.0 (file transfer) |

Table 7: Object Identifier Values

Note: Above OID values for basic and extended IA5 Text Body Part Types, Bilaterally Defined Body Part Type and File Transfer Body Part Type

are derived from ISO/IEC 10021-7 [9]. The AMHS CS [1] describes indication for support of the AMHS Functional Group FTBP through inclusion of the above OID value in the attribute type *mhs-exclusively-acceptable-eits*. For the General Text Body Part Type above OID values are derived from ICAO Doc 9880 Part II [2]. Use of Bilaterally Defined Body Part Type is discouraged and not supported by AMC.

7. Trouble Shooting

This chapter provides considerations and advice for trouble shooting.

There are several potential reasons in case the communication between the Central European DSA and a Co-operating or Adjacent DSA is not working as expected. This chapter lists a number of sources for malfunction and tools in support of the analysis.

The listings and examples in this chapter do not claim to be complete, however provide starting points and a selection of tools that might be useful.

7.1 Sources of Malfunction

A failure to establish an association through a bind operation or the disruption of service between the Central European DSA and the Co-operating or Adjacent DSA is getting visible only in case one of the involved parties tries to establish communication for the exchange of information. The bind operation or a subsequent shadowing or chaining operation could fail.

Following reasons are potential main sources of malfunction of the overall service:

- The underlying network is not available.
It is not possible to establish communication at the network level and a VPN could not be established.
- The Co-operating or Adjacent DSA is not available.
The Co-operating or Adjacent DSA does not initiate or does not respond to requests.
- The Central European DSA is not available.
The Central European DSA does not initiate or does not respond to requests.
- The Central European DSA, the Co-operating or Adjacent DSA refuses communication.
There is a misconfiguration at least at one of the communication peers.
- The information available in the Co-operating or Adjacent DSA is not up-to-date. The most recent shadowing or chaining operations failed.
- The information is invalid and has been distributed to Co-operating and Adjacent DSAs.

7.2 Analysis

This section describes approaches for analysis in case of malfunction. The approaches make use of the Directory System Agent, Directory User Agent or

tools which might be available from a second source. The following description does not claim to be complete, but provides starting points.

7.2.1 Directory System Agent

Most implementations of Directory System Agents (DSAs) provide a Human-Machine-Interface for configuration and management of the DSA. Using this HMI, it should be possible to determine the operational status of the DSA and to check the communication setup between the peers.

Logging information provided in a database or a log file can also serve as input for analysis.

Please note the availability of management capabilities and logging information depends on the implementation and on the potential configuration options.

7.2.2 Directory User Agent

A simple method to check the operational status of a DSA is to bind to the DSA using a Directory User Agent (DUA).

By means of the DUA it is also possible to check the contents of the EDS, i.e. of the contents available at the local, Co-operating or Adjacent DSA.

7.2.3 Network Analysis Tool

Using a packet analyser, also known as network analyser, protocol analyser or packet sniffer, it is possible to analyse the data streams across the network, to identify whether communication between the peers appears in general and to analyse in depth the exchanged packets at the different layers up to the application layer. Some tools allow to record or capture packet exchanged over the network.

A variety of tools with distinct capabilities, under different licenses and at variable costs is available. The tool of choice should be able to decode packets not only at the transport layer but also up to the application layer and should be able to display the contents of Application PDUs in a human readable form.

Wireshark, formerly known as Ethereal, is just one example for a free of cost packet analyser published under the GNU General Public License (GNU GPL). Another non-commercial tool is for example tcpdump. There are also several commercial products available.

END OF DOCUMENT