EUR AMHS Manual

Appendix G

European Directory Service	
Document Reference:	EUR AMHS Manual, Appendix G
Author:	EUROCONTROL, ICAO AFSG PG
Revision Number:	Version 9.0
Date:	10/04/14
Filename:	EUR_AMHS_Manual-Appx_G-v9_0.doc

Document Control Log

Edition	Date	Comments	Section/pages affected
0.1	19/03/2012	Creation of the document.	all
0.2	27/06/2012	Attachment of CP-AMHSM-12-005 (EUR AMHS Manual, Appendix G)	all
0.3	11/09/2012	Incorporation of comments from Greece, EUROCONTROL and Germany	all
0.4	15/02/2013	Alignment of X.500 DAP terminology, establishment of context, editorial changes	all
1.0	08/03/2013	Finalised version for presenting to AFSG/17 as attachment of CP-AMHSM-12-005	all
8.0	25/04/2013	Adopted version (AFSG/17) (no other versions in between)	
8.1	12/03/2014	Incorporation of CP-AMHSM-13-010	6.3.1, 6.3.2, 6.4.2
9.0	10/04/2014	Adopted version (AFSG/18)	

Table of contents

References

[1] 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, latest version

[3] ICAO EUR Doc 021 ATS Messaging Management Manual, latest version

[4] ICAO EUR Doc 022 EUR AFS Security Guidelines, latest version

[5] ICAO Doc 9880 AN/466 Manual on Detailed Technical Specifications for the Aeronautical Telecommunication Network (ATN) using ISO/OSI Standards and Protocols, Part I — Air-Ground Applications, 1st Edition, 2010

[6] 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

[7] ICAO Doc 9880 AN/466 Manual on Detailed Technical Specifications for the Aeronautical Telecommunication Network (ATN) using ISO/OSI Standards and Protocols, Part III — Upper Layer Communications Service (ULCS) and Internet Communications Service (ICS), 1st Edition, 2010

[8] 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

[9] ICAO Doc 9896 Manual on the Aeronautical Telecommunication Network (ATN) using Internet Protocol Suite (IPS) Standards and Protocols, 1st Edition, 2010

[10] 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.

[11] IETF RFC 4511 Lightweight Directory Access Protocol (LDAP): The Protocol, June 2006

[12] IETF RFC 2849 The LDAP Data Interchange Format (LDIF) - Technical Specification, June 2000

[13] IETF RFC 1006 ISO Transport Service on top of the TCP, Version 3, May 1987

[14] IETF RFC 2126 ISO Transport Service on top of TCP (ITOT), March 1997

[15] European Directory Service (EDS) Operational Concept – WP1 (Analysis), Version 1.0, October 2011

[16] European Directory Service (EDS) Operational Concept – WP2 (Concept), Version 1.0, October 2011

Table of Figures

List of Tables

1 Introduction

1.1 Scope of the Document

1.1.1 This document constitutes the specification of the European Directory Service (EDS) Operational Concept, describing how the EDS should be used as a common European facility in support of ATN applications and AMHS in particular.

1.1.2 The specification laid down in the EUROCONTROL EDS concept document [16] was developed in the framework of the EUROCONTROL EDS Operational Concept study and handed over to the ICAO AFSG for consideration, subsequent adoption and maintenance thereafter. The AFSG decided to incorporate the specification into the EUR AMHS Manual as an Appendix.

1.2 Purpose of the Document

1.2.1 The purpose of this document is to provide a comprehensive analysis of the various aspects of the solution for the European Directory Service. Besides technology considerations, the document addresses operational, cooperation and transitional issues.

1.2.2 The document aims to give advice in support of the implementation and operations of the European Directory Service. The major focus is set on the exchange of information at the international level. Distribution of information at national or local levels and access to information by Directory users are taken into account to give the full picture, however they are considered local implementation matters.

1.3 Structure of the Document

1.3.1 This document consists of the following chapters:

- Chapter 1 (this chapter) provides an introduction to the document.
- Chapter 2 gives the overall picture from the topology point of view.
- Chapter 3 discusses the refinement of functional objects.
- Chapter 4 outlines the X.500 protocols to be used for exchange of information between functional objects.
- Chapter 5 describes the concept of operation including aspects of cooperation with Regions, States and Organisations not participating in the concept.
- Chapter 6 looks at the schema definition.
- Chapter 7 considers transition and migration towards the European Directory Service.
- Chapter 8 discusses capacity and performance considerations with respect to the implementation of the European Directory Service.
- Chapter 9 outlines future options of the European Directory Service.

2 Overall Topology

2.1 The European Directory Service (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.

2.2 The AMHS CS makes reference to ICAO EUR Doc 020 [2] and ICAO Doc 9880 Part IV [8]. ICAO Doc 9880 Part IV describes the ATN Directory service, in particular the functional objects, protocols and schema definition with respect to the X.500 base standards [9].

2.3 ICAO EUR Doc 020 indicates in Annex K of Appendix B, the directory information needed to support the AMHS.

2.4 The AMHS CS describes an architecture with the Directory System Agents (DSA) of the various Directory Management Domains (DMDs) connected to one central DSA. The role of the central DSA is to collect data from participating States and Organisations as well as from Regions, States and Organisations not directly participating in the concept; to check consistency of the collected data, and to provide validated data to States and Organisations. With regard to the ATS Messaging Management process, ICAO EUR Doc 021 [3] contains a detailed description.

2.5 The EDS analysis [15] confirms the centralised approach of the AMHS CS [1] in order to implement a Directory service as a Common Facility in the European area. The EDS Operational Concept describes the exchange of information at the international level between the participating States and Organisations with regard to the overall topology, used protocols, data structures, workflow, and procedures. The European Directory Service (EDS) is expected to support the various ATN applications, especially the AMHS in implementation of the Extended ATS Message Handling Service. The EDS Operational Concept also describes the protocols used by Directory users for access to the information stored in the Directory. Further aspects of access by users and national respective local distribution of information are considered out of scope of the EDS Operational Concept.

2.6 In addition to a pure 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 Organisations not participating in the concept also provide data that is required by the participating States and Organisations as well as vice versa.

2.7 The EDS Operational Concept describes an overall online Directory solution.

2.8 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 takes place on demand or by schedule, but without manual initiation or intervention by human users. A permanent connection on a 24 hour basis is not implied by the term online.

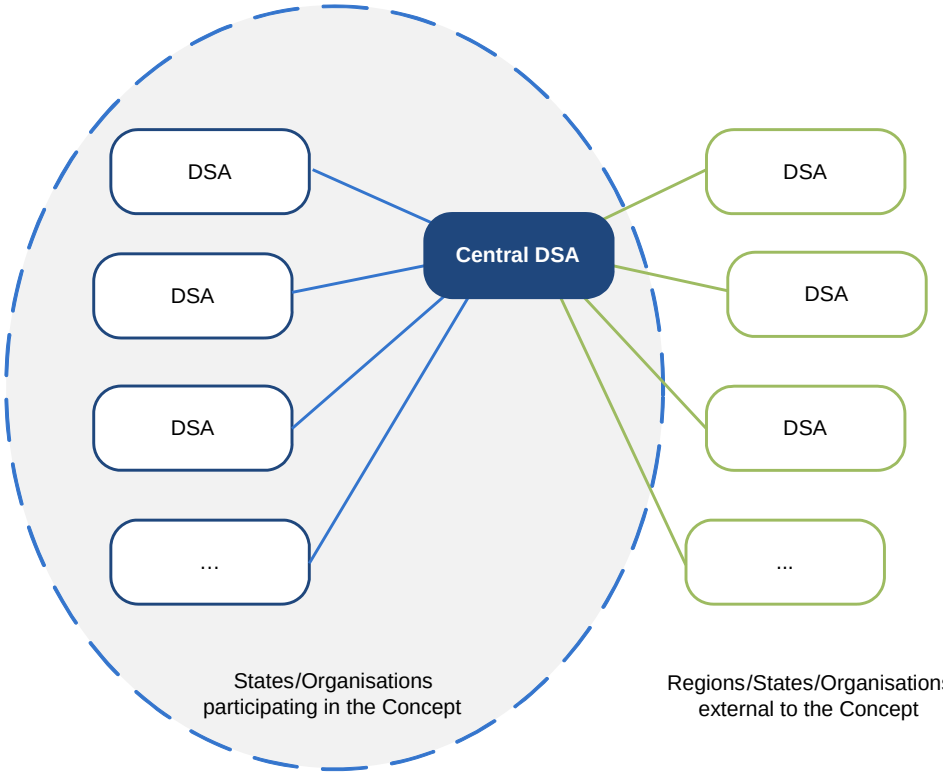

Figure 1: Participating and non-participating Directory Management Domains

2.9 The EDS Operational Concept specifies the cooperation of the central DSA with the DSAs in the participating and non-participating DMDs. These DMDs might implement further, subordinate DSAs in support of geographical deployment, quality of service, redundancy, 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 the DMDs are therefore considered out of scope in the context of the concept.

3 Functional Objects

3.1 Relationship to Base Standards and Doc 9880

3.1.1 The functional model of the ATN Directory service as per ICAO Doc 9880 Part IV [8] refines the basic, functional model given by the X.500 base standards [10], which is further refined by the EDS Operational Concept.

3.2 Directory System Agent

3.2.1 A Directory System Agent (DSA) is a functional object in the model of the ATN Directory service.

3.2.2 According to the X.500 model, a DSA provides access to the information stored in the Directory for other DSAs and users.

3.2.3 A DSA within the EDS Operational Concept implements one of the following profiles according to the function of the respective DSA:

- Central European DSA; or
- Co-operating DSA; or
- Adjacent DSA.

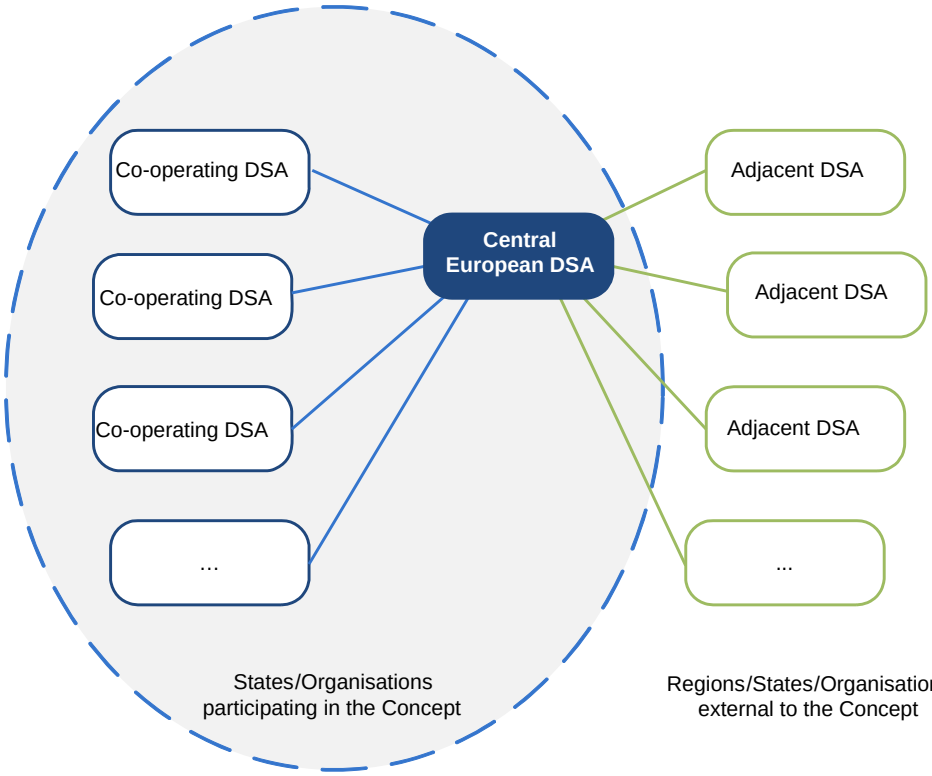

Figure 2: Directory System Agents within the EDS Operational Concept

Central European DSA

3.2.4 The Central European DSA is implemented as a Common Facility within the European Directory Service (EDS).

3.2.5 The role of this facility is to:

- collect data from participating States and Organisations;
- collect data from non-participating Regions, States and Organisations;
- apply a workflow mechanism;
- ensure consistency of collected data;
- provide overall validated data to participating States and Organisations; and
- provide validated data with regard to participating States and Organisation to non-participating Regions, States and Organisations.

Note.– The amount of data collected from and provided to a DSA depends on the profile implemented by the DSA.

3.2.6 With regard to non-participating Regions, States and Organisations, the Central European DSA acts on behalf of the Co-operating DSAs. In this respect, there is no need for a Co-operating DSA to exchange data with any other DSA, but the Central European DSA.

Co-operating DSA

3.2.7 A Co-operating DSA participates in the concept and contributes to the overall functions within the European Directory Service.

3.2.8 The role of this facility is to:

- allow users to modify local data;
- provide local data to the Central European DSA;
- receive validated data provided by the Central European DSA; and
- provide validated data to subordinate DSAs and local users.

3.2.9 The validated data received from the Central European DSA covers data collected from any other Co-operating or Adjacent DSA.

Adjacent DSA

3.2.10 An Adjacent DSA does not directly participate in the concept; however it provides data to and receives data from the Central European DSA.

3.2.11 The role of this facility is to:

- provide local/regional data to the Central European DSA and
- receive a part of the validated data provided by the Central European DSA.

Note.– The above listing identifies only a minimum set of profiles in order to enable exchange of data with the Central European DSA.

3.2.12 The part of the validated data received from the Central European DSA covers data collected from all Co-operating DSAs on whose behalf the Central European DSA acts.

3.2.13 Any other Region, State or Organisation may operate an Adjacent DSA.

3.3 Directory User Agent

3.3.1 A Directory User Agent (DUA) is a functional object in the model of the ATN Directory service.

3.3.2 Services available at a DUA are provided by the Directory in response to operations initiated by a human or system user. There are operations to allow interrogation of the Directory and others to allow modifications.

3.3.3 A DUA within the EDS Operational Concept implements one of the following profiles according to the function of the respective DUA:

- Administrative DUA
- Operational Personnel DUA
- Autonomous Operational DUA

Note.– The profiles of the previous three DUA types are specified in ICAO Doc 9880 Part IV [8].

- Central Administrative DUA

Administrative DUA

3.3.4 An Administrative DUA provides the user with the full range of Directory operations and is suitable for Directory administrators of various kinds. It needs access to all of the Directory operations, and it is subject to access controls for the modification operations. It is also required to protect the integrity and accuracy of the data held in the Directory Information Base (DIB).

Operational Personnel DUA

3.3.5 An Operational Personnel DUA provides a (human) operational user with the limited range of Directory operations enabling interrogation of the Directory without being granted access to the modification operations. Typical users of Operational Personnel DUAs include operators of systems in the ATN, AMHS users and users of end systems supporting other ATN applications. Planners and management personnel also belong to this profile. This DUA requires guarantees of data integrity and accuracy.

Autonomous Operational DUA

3.3.6 An Autonomous Operational DUA (supporting, for example, AMHS MTAs, UAs, MS and MTCUs, or other ATN applications) is an autonomous process with limited requirements of Directory interrogation operations (e.g. it requires the read, compare and search operations only) and it operates without human intervention to invoke Directory operations and evaluate results. This DUA requires guarantees of data accuracy.

Central Administrative DUA

3.3.7 The Central Administrative DUA is an Administrative DUA as specified by ICAO Doc 9880 Part IV [8] designed to provide the user with workflow capabilities in order to implement the ATS Messaging Management process at the Central European DSA. A typical

user of the Central Administrative DUA is the administrator of the Central European DSA in charge of consistency and validation of the collected data.

4 Protocols

4.1 The X.500 Directory base standards define protocols for communications between the functional objects:

- Directory System Protocol (DSP)
- Directory Information Shadowing Protocol (DISP)
- Directory Access Protocol (DAP)
- Directory Operational Bindings Management Protocol (DOP)

Note.– In the context of the European Directory Service, DOP is considered out of scope as already stated by the AMHS Community Specification [1].

4.2 DSP supports communications between two DSAs, where a request cannot be fully resolved by one DSA and forwarded to one or more other DSAs through chaining. Use of referrals is discouraged by the EDS Operational Concept as it increases the number of access points for the users' DUAs. Use of DSP for chaining is recommended.

4.3 DISP supports shadowing between two DSAs where a copy of data is made available at another DSA. Use of DISP reduces the dependency from underlying international networks and facilitates the holding of data close to the user. Use of DISP for shadowing is recommended.

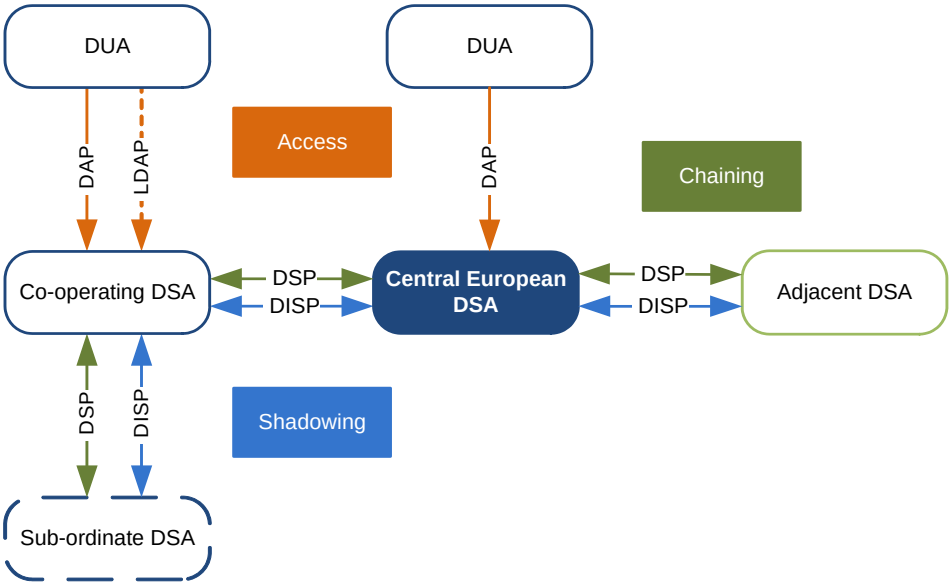

Figure 3: European Directory Service communications protocols

4.4 DAP is used by DUAs in order to enable users to access the European Directory Service. Depending on the access rights, the user can access data in the Directory Information Base (DIB) and perform operations.

4.5 The available DAP operations fall in two categories as specified in the X.500 base standards [10]:

- Interrogation operations which allow to query the Directory; and
- Modification operations which apply changes to the Directory.

4.6 Using DAP the X.500 base standards specify the following operations for Directory interrogation:

- *Read* to determine the attributes of an entry and related values;
- *Compare* to check whether a supplied value matches a value of a particular attribute of a particular entry;
- *List* to receive a list of immediate subordinates of a particular entry;
- *Search* to identify entries in portions of the Directory that satisfy a supplied filter; and
- *Abandon* to inform the Directory that the initiating user of a previous interrogation operation is no longer interested in the operation being carried out.

4.7 Using DAP the X.500 base standards specify the following operations for Directory modification:

- *Add entry* to insert a new leaf entry;
- *Remove entry* to delete an existing leaf entry;
- *Modify entry* to apply a sequence of changes to a particular entry; and
- *Modify distinguished name* to change the relative distinguished name of a particular entry.

4.8 Use of DAP is recommended for management purposes and is proposed for other purposes depending on the needs of the respective applications.

4.9 In addition to DAP specified by ICAO Doc 9880 Part IV [8] for access by Directory users, Operational Personnel DUA and Autonomous Operational DUAs of end users with limited needs may make use of the Lightweight Directory Access Protocol (LDAP) [11].

4.10 LDAP was developed as an alternate, simpler means to access a Directory compared to DAP, aiming to provide equivalent operations. In contrast to previous versions, the current version 3 of LDAP (LDAPv3) supports peer authentication, which is considered essential in the context of ATN Directory and EDS. Use of LDAPv3 is optional for end users with limited needs.

Note.– LDAPv3 does not support read and list operations.

4.11 An ATN application accessing the Directory shall make use of either DAP or LDAPv3.

Note.– LDAP provides alternate access to an X.500 Directory by protocol means. Support of LDAP by COTS X.500 DSAs is widely available. For the exchange of information between DSAs, the use of X.500 protocols is recommended.

4.12 At the transport layer, the implementations of Directory protocols can make use of an OSI lower layer stack. However, in the light of emerging European network infrastructure, it is proposed to implement a transport mapping from the OSI transport layer to the Transmission Control Protocol (TCP) similar to the transport mapping for the AMHS in the

EUR Region as specified by ICAO EUR 020 [2]. Such a transport mapping implements RFC 1006 [13] or RFC 2126 [14] for Internet Protocol Versions 4 (IPv4) or 6 (IPv6) respectively. ICAO Doc 9896 [9] adopted IPv6 for the Aeronautical Telecommunication Network. The transport mapping onto TCP and the use of IP would allow the use of available, international IP-based network infrastructure in Europe.

Note.– Support of transport mapping from OSI transport to TCP using RFC 1006 or RFC 2126 as well as support of IPv4 and IPv6 by X.500 COTS products is widely available.

5 Concept of Operation

5.1 Relationship to Doc 9880

5.1.1 ICAO Doc 9880 Part IV [8] specifies technical aspects of the ATN Directory service such as DIT structure, objects classes, attribute types, protocols, etc. However, the specification does not address operational aspects given in this chapter.

5.2 Roles

5.2.1 In terms of management of the European Directory Service (EDS), the EDS Operational Concept identifies the following roles:

- Central administrator
- Co-operating operator
- Adjacent operator
- End User

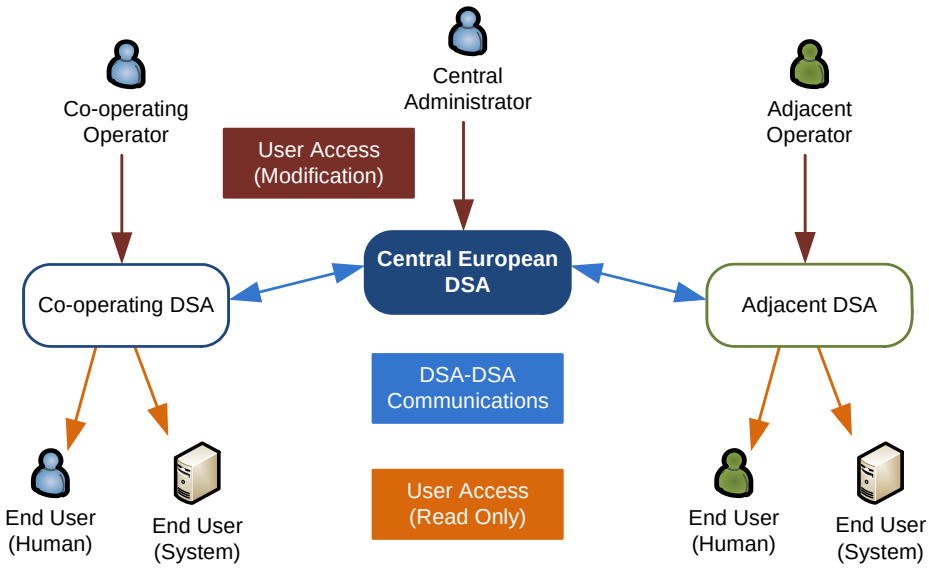

Figure 4: Interaction of European Directory Service roles

Central Administrator

5.2.2 The Central Administrator is in charge of systems management of the Central European DSA. The Central Administrator manages the connections to the other DSAs and controls access to data mastered by the Central European DSA. Furthermore he manages global data mastered by the Central European DSA.

5.2.3 The Central Administrator uses a Central Administrative DUA and performs workflow operations. He validates data ensuring consistency of data mastered by the Central European DSA. The Central Administrator can perform interrogation and modification operations to global data and Managed Data as well as interrogation operations to all other data.

Co-operating Operator

5.2.4 The Co-Operating Operator is in charge of management of data provided by the respective State or Organisation participating in the concept.

5.2.5 For management of local data mastered by the Co-operating DSA, the Co-operating Operator accesses the local DSA. For management of data mastered by the Central European DSA, the Co-operating Operator accesses the local DSA and the local DSA forwards the request to the Central European DSA for processing of the request.

5.2.6 The Co-operating Operator uses an Administrative DUA and can perform interrogation operations to all data and additionally modification operations to the data he manages.

Adjacent Operator

5.2.7 The Adjacent Operator fulfils a task similar to Co-operating Operator.

5.2.8 The Adjacent Operator uses an Administrative DUA and can perform interrogation and modification operations to data he manages, as well as interrogation operations to data replicated by the Central European DSA. However the Adjacent Operator typically does not directly access the Central European DSA.

End User

5.2.9 End Users are consumers of Directory data and can perform interrogation operations to the Directory. Modification operations by End Users are not permitted.

5.2.10 End Users are either human or machine/system users. Human users utilise an Operational Personnel DUA whereas system users make use of an Autonomous Operational DUA.

5.2.11 Human end users are for instance direct AMHS users and operators of ATN applications making use of the Directory service. Typical system users are components of ATN applications such as the AFTN/AMHS Gateway and the ATS Message User Agent with only limited requirements. Access of system users is restricted to interrogation operations and to sub-trees as required in order to implement the specified function. The ATS Message Server can also appear as a system user to the Directory service; however the use of Directory by the ATS Message Server is not specified by ICAO Doc 9880 Part II [6] and thus is considered a local implementation matter. Nevertheless ICAO Doc 9880 Part IV [8] contains objects classes appropriate for use by the ATS Message Server.

Relations to AMC User Categories

5.2.12 Due to the differences in nature of EDS and AMC, the roles of EDS cannot be mapped directly onto the user categories of AMC identified by ICAO EUR Doc 021 [3]. However, similar tasks are assigned to EDS roles and AMC user categories, that allow the following comparison at an abstract level.

EDS Role	**AMC User Category**
Central Administrator	AMC Operator

EDS Role	AMC User Category
Co-operating Operator	CCC Operator
Adjacent Operator	External COM Operators
End User (Human)	AMF-I Users
End User (Human)	Read/Only Users
End User (System)	n/a (Access by systems not intended)
n/a (Concept restricted to active roles)	Participating COM Centres

Table 1: EDS Roles and AMC User categories

5.3 Flow of Data

5.3.1 Collection and Distribution of Information

5.3.1.1 In order to make relevant information locally available, the EDS Operational Concept proposes to provide copies of information by replication. Replication between DSAs in the framework of the European Directory Service appears in two situations: collection and distribution of information. Collection is needed for information not hosted by the Central European DSA, which, nevertheless, is intended to be provided to States and Organisations. Distribution is used to provide a copy of information to States and Organisations.

5.3.1.2 The X.500 base standards [9] specify the Directory Information Shadowing Protocol (DISP) for replication of information. Also, the AMHS CS [1] mentions DISP for replication. Consequently the EDS Operational Concept proposes to make use of DISP for the purpose of collection and distribution of information.

5.3.1.3 However, taking into account available products, existing systems and the fact, that DISP was not mandated by the above documents, the EDS Operational Concept explicitly allows for other, non-standard or proprietary means of collection and distribution.

5.3.1.4 Within the context of the European Directory Service, collection and distribution is performed in one of the following forms:

- Push collection/distribution
- Pull collection/distribution

Push Collection/Distribution

5.3.1.5 Collection and Distribution is driven by the Central European DSA. The DSAs perform replication by protocol means using DISP (shadowing). For collection and distribution of information, the Central European DSA initiates push replication.

Pull Collection/Distribution

5.3.1.6 Collection and Distribution is driven by a dedicated, non-standard application such as a specialised DUA or a script interfacing the DSA. Data is collected and distributed over protocol e.g. Directory Access Protocol (DAP) and Directory System Protocol (DSP). For collection of information, the Central European DSA initiates pull collection. For distribution of information, the Co-operating respectively Adjacent DSA initiates pull distribution.

5.3.1.7 The flow of data between the involved DSAs depends on the nature of the data. Within the European Directory we find two types of data:

- Shared Data
- Managed Data

5.3.1.8 Managed Data allows for central management and control of data (e.g. for address management data) whereas Shared Data is handled in a distributed way (e.g. white pages).

5.3.2 Shared Data

5.3.2.1 Shared Data is maintained in a decentralised manner using a replicated topology to populate the Central European DSA with the data. The Central European DSA makes the overall data available to each State and Organisation through a distributed topology.

5.3.2.2 Each Co-operating and Adjacent DSA masters the respective part of the Shared Data, i.e. the master copy of the data is hosted by the local DSAs. The Co-operating and Adjacent Operators apply modifications to their part of the Shared Data through the Administrative DUA accessing the local DSA by means of DAP.

5.3.2.3 Workflow mechanisms do not apply to Shared Data since it is maintained in a decentralised manner.

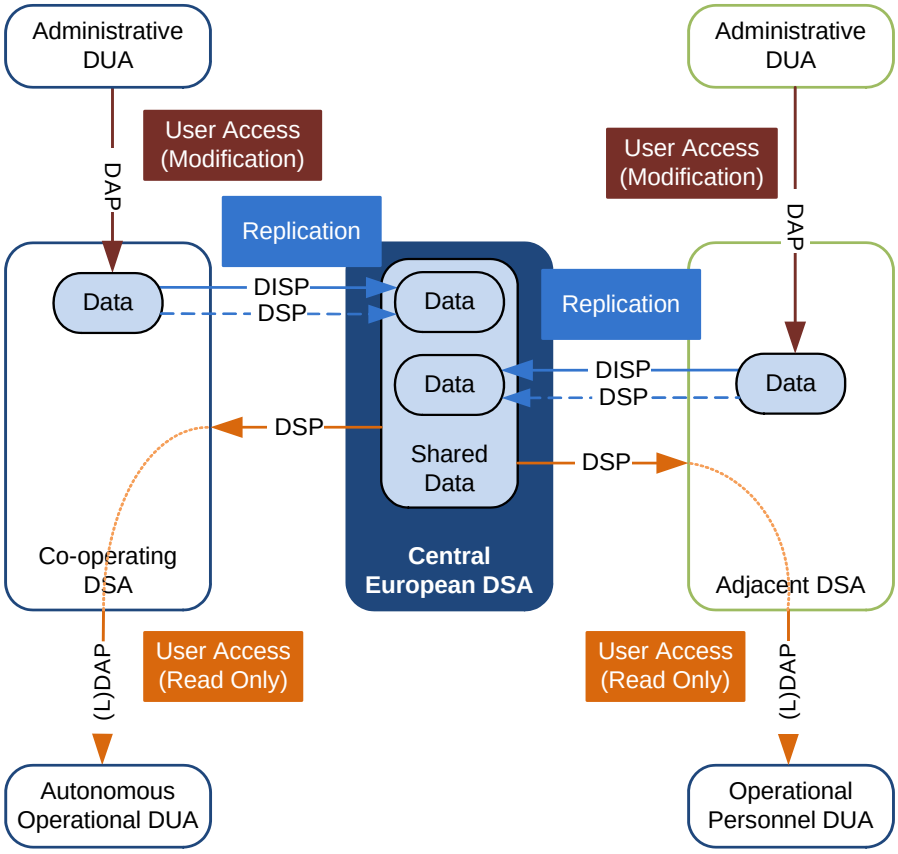

Figure 5: Decentralised maintenance of Shared Data

5.3.2.4 The parts of Shared Data hosted by Co-operating and Adjacent DSAs are replicated to the Central European DSA by means of DISP. Where DISP is not available at a Co-Operating or Adjacent DSA, the Central European DSA provides a collecting mechanism based on DSP. At the Central European DSA the overall data collected from Regions, States and Organisations is available for retrieval. The Central European DSA allows the Shared Data to be accessed by every Region, State or Organisation using chaining. As data is shadowed to the Central European DSA, the change can be instantly observed by other DSAs.

5.3.2.5 End Users within Regions, States and Organisations access the data through their local DSA by means of the DAP. LDAP may be used instead of DAP for access by human users or applications with limited needs. Human and system End Users perform interrogation operations only. The local DSAs forward the requests initiated by the End Users to the Central European DSA by means of the DSP (chaining). Access to the local DSA provides a single access point to End Users.

5.3.3 Managed Data

5.3.3.1 Managed Data is centrally maintained, validated and supplied to other Regions, States and Organisations based on a centralised and replicated topology. Managed data is subject to workflow mechanisms and supports different sets of data, also referred to as versions of data.

5.3.3.2 The Central European DSA masters the Managed Data, i.e. the master copy of the data is hosted by the Central European DSA. Mastered Data includes data collected from participating and non-participating Regions, States and Organisations. Co-operating DSAs apply modifications to Mastered Data through their Administrative DUAs accessing their local DSAs by means of the DAP. The local DSAs forward the request to the Central European by

means of the DSP (chaining). Adjacent Operators apply modifications to their local data mastered by the Adjacent DSA. The Central European DSA receives Managed Data from Adjacent DSAs through collection means.

5.3.3.3 The Adjacent DSA then replicates the local data to the Central European DSA by means of DISP (shadowing). In case DISP is not available at an Adjacent DSA, the Central European DSA provides a collecting mechanism based on DSP. Access to the local DSA provides a single access point to End Users.

5.3.3.4 Since all of the Managed Data is available at the Central European DSA, it is possible to apply a workflow mechanism modelled according to ATS Messaging Management process. The workflow mechanism applied through the Central Administrative DUA allows for a controlled way of collection, validation, management, versioning, and distribution on a time cycle basis. However, it needs to be applied on top of standard Directory systems interfacing with the Central European DSA. On approval, the consistent and validated data is copied to the appropriate sub-tree for distribution.

5.3.3.5 The Central European DSA replicates the consistent and validated data to the Co-operating and Adjacent DSAs by means of the DISP. In case DISP is not available at a Co-Operating or Adjacent DSA, the Central European DSA provides access to the Managed Data by means of DSP. The amount of data replicated to the DSAs depends on the respective role. Co-operating DSAs receive a full copy of the Managed Data including data collected from participating and non-participating Regions, States and Organisations.

5.3.3.6 Adjacent DSAs receive only a portion of the Managed Data. The data replicated to Adjacent DSAs is restricted to the data collected from the Co-operating DSAs. Data originating from Regions, States and Organisation not participating in the concept is not replicated to Adjacent DSAs. Further restriction could be applied to distribution on a per DSA basis.

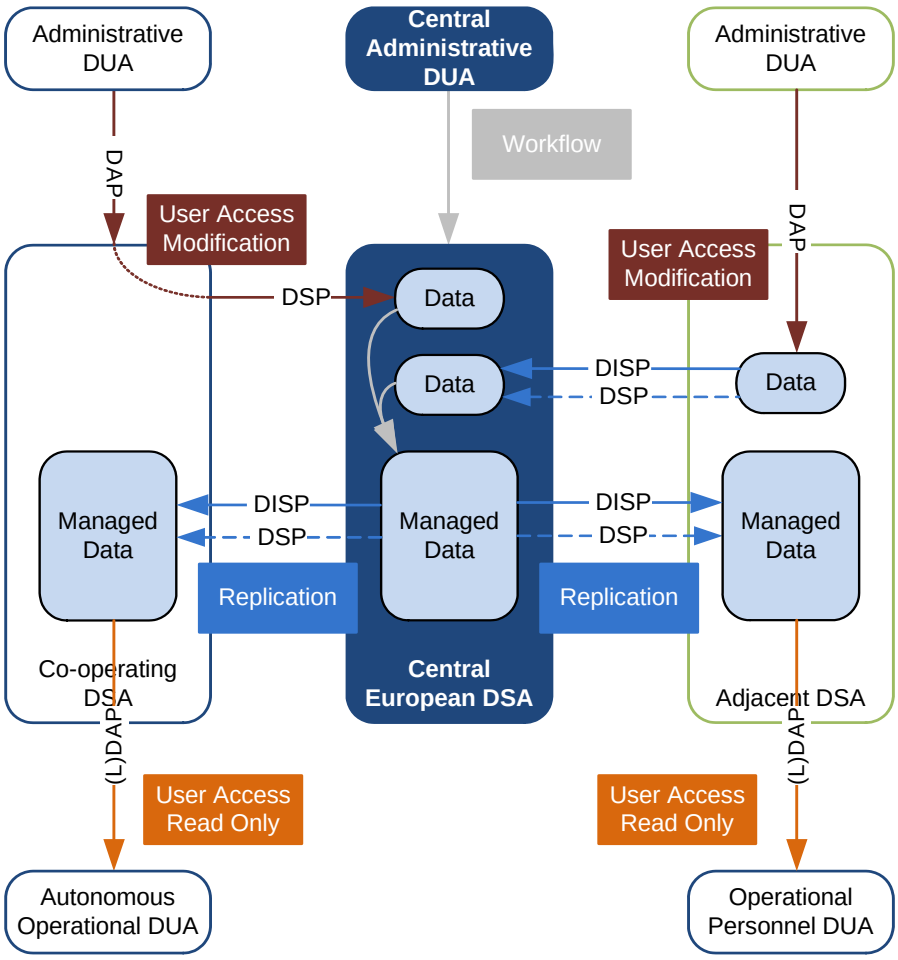

Figure 6: Centralised maintenance of Managed Data

5.3.3.7 End users within Regions, States and Organisations access the replicated data at their local DSAs using DAP. LDAP may be used instead of DAP for access by human users or applications with limited needs. Human and system End Users perform interrogation operations only. Modification operations are not permitted to End Users.

5.3.4 Managed Data Areas

5.3.4.1 Different versions of information are supported by distinct areas containing a complete set of information. The Managed Data consists of three areas for management of data using the workflow mechanism:

- Background Area
- Pre-operational Area
- Operational Area

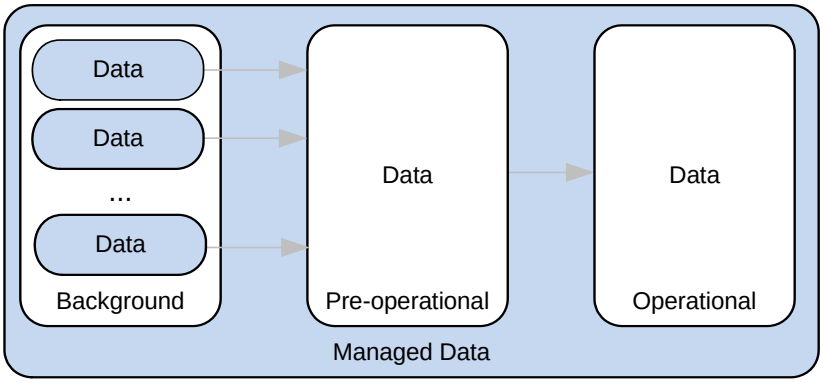

Figure 7: Managed Data areas

Background Area

5.3.4.2 The background area is intended for collection and management of information. The background area comprises parts of information provided by different sources and by different means.

5.3.4.3 Information provided by Co-operating States and Organisations is hosted in this area and accessible for management by Co-operating Operators. Information provided by Adjacent States and Organisations is hosted by Adjacent DSAs and replicated by schedule to make it available in the background area. Data of Bodies, States, and Organisations, that do not provide their data by protocol means, is hosted at the Central European DSA and maintained by the Central Administrator on behalf of the respective Body, State, or Organisation.

5.3.4.4 Bodies, States and Organisations without a local Directory infrastructure might manage their data through a web interface if implemented by the Central European DSA.

Pre-operational Area

5.3.4.5 The pre-operational area is intended for distribution of information prior to becoming effective. The information in the pre-operational area is a copy of the parts of information in the background area and remains available and unchanged until the next cycle. Distribution of information beforehand allows States and Organisations to prepare legacy systems that will not be able to retrieve the information from the European Directory Service using an Autonomous Operational DUA and to take measures in line with local policy.

5.3.4.6 In case a Co-operating or Adjacent DSA does not support push distribution using DISP, the information is also available for pull distribution beforehand in order to have the information already available when it receives operational status.

Operational Area

5.3.4.7 The operational area is intended for distribution of effective information.

5.3.4.8 Distribution of information in the operational area makes effective information available to users and systems at the predetermined time. The information in the operational area is a copy of the pre-operational area and remains available and unchanged until the next cycle.

Note.– When pull distribution is used, the Co-operating or Adjacent Operator is responsible to initiate the action at the predetermined times.

5.3.5 Managed Data in Support of the ATSMHS

5.3.5.1 Derived from the ATS Messaging Management process, the EDS Operational Concept proposes to apply the workflow mechanism in support of the ATSMHS.

5.3.5.2 The following elements are put under the control of Managed Data:

- AMHS MD Register with object class atn-amhsMD;
- CAAS mapping information with object class atn-organization;
- User information with object class atn-amhs-user; and
- AMHS user capabilities with object class atn-amhs-user.

5.3.5.3 The workflow mechanism may be applied to further elements depending on the requirements of the respective applications.

5.4 Procedures

5.4.1 AMC Procedures

5.4.1.1 ICAO Doc 9880 Part IV [8] specifies various technical aspects of the ATN Directory service, however does not address organisational and procedural details. With respect to AMHS address management and management of further data such as network inventory, routing directory, collection of statistics, etc., ICAO EUR Doc 021 (ATS Messaging Management Manual) [3] describes procedures known as the *AMC Procedures*.

5.4.1.2 In the context of this concept, functions of the AMC partially overlap with functions of the ATN Directory service. Both deal with AMHS-related information in support of management of users and address conversion. Even though some services of AMC might need to be migrated to Directory services, it is not the intention of the EDS Operational Concept to promote the replacement of further functions of AMC.

5.4.1.3 The ATS Messaging Management Manual [3] identifies *Co-operating COM Centres* and *External COM Centres* as involved entities. Co-operating COM Centres participate in the ATS Messaging Management as a whole and adhere to its specification, whereas External COM Centres participate in a limited way only.

5.4.1.4 The AIRAC (Aeronautical Information Regulation And Control) cycle as given by the ATS Messaging Manual [3] is used to collect, validate acknowledge and publish information. One cycle lasts 28 days and is split into five phases. In order to allow parallel operation of AMC and European Directory Services during transition, the establishment of aligned procedures for EDS is required.

5.4.1.5 No dedicated procedures are associated with Shared Data. Information is replicated on change by DISP making it immediately visible at the Central European DSA. Distribution to the Central European DSA using DSP is performed daily at 11:00 UTC in order to limit the effort for the pull mechanism performed by the Central European DSA.

5.4.1.6 For the Managed Data the EDS Operational Concept adopts the basic concept of the 28 day AIRAC cycle. The duration of cycles might be adjusted in coordination with the ATS Messaging Management process or after completion of the transition to the European Directory Service. To ease transition and to support parallel operation of AMC, the phases in the EDS are strictly aligned to the description of the AIRAC cycle in the ATS Messaging

Management Manual [3], including the breakdown of days. In contrast to the AMC procedures, procedures in the EDS offer a high level of automation, which is synchronised at 11:00 UTC. I.e. Preparatory actions have to be completed by 11:00 UTC in order to allow automated processes to start at 11:00 UTC.

5.4.2 Five AMC phases within the AIRAC cycle

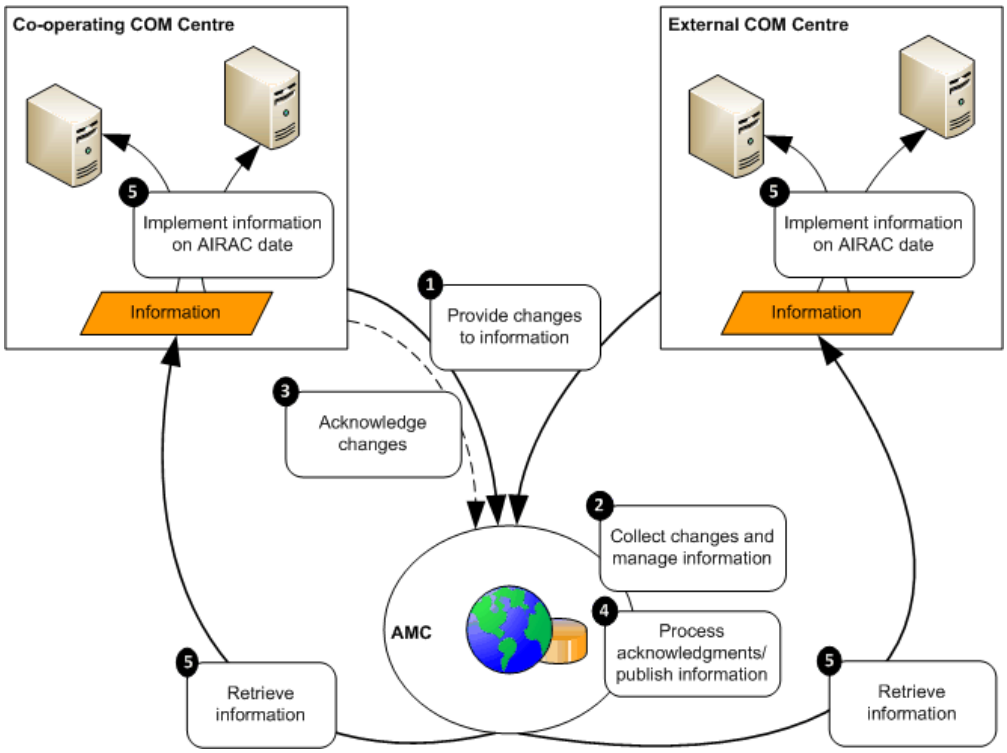

Figure 8: Phases within the AIRAC cycle

5.4.2.1 Data Entry Phase

Period:	Phase starts day 1, ends day 7.
Area involved:	Background.
Co-operating/Adjacent Operator tasks:	Perform interrogation and modification operations to the background area of the Managed Data in order to maintain data.
Central Administrator tasks:	Perform interrogation and modification operations to the background area of the Managed Data in order to maintain data.

5.4.2.1.1 Co-operating Operators, in charge of managing States' or Organisations' information perform interrogation and modification operations to the respective part of the background area hosted by the Central European DSA. Adjacent Operators perform interrogation and modification operations at their local DSA.

5.4.2.1.2 Changes applied at Adjacent DSAs are not immediately visible at the Central European DSA. The Central Administrator performs interrogation and modification operations to information he manages on behalf of Bodies, States and Organisations, that do not provide their data through Directory services.

5.4.2.1.3 At the end of this phase, the data provided by Regions, States and Organisation is up to date.

5.4.2.1.4 During the transition period the EDS Operational Concept proposes additional means for States and Organisations that do not participate directly in Directory services by implementing a DSA. In this situation the Central European DSA hosts the information on behalf of the respective States and Organisations.

5.4.2.1.5 There are several possibilities to allow for management of the State's or Organisation's information in the background area of the Managed Data.

5.4.2.1.6 Further transitional considerations are provided in Chapter 7.

5.4.2.2 Data Validation and Processing Phase

Period:	Phase starts day 8, ends day 14.
Area involved:	Background and pre-operational.
Co-operating/Adjacent Operator tasks:	Coordinate with Central Administrator as necessary. Initiate distribution of data, if triggered manually.
Central Administrator tasks:	Initiate collection of data from Adjacent DSAs, if triggered manually. Validate data and coordinate with Co-operating/Adjacent Operator as necessary. Make overall data available in pre-operational area.

5.4.2.2.1 The data validation and processing phase is used to collect information from Adjacent DSAs, to validate the overall data in the background area, and to provide validated overall data to the pre-operational area.

5.4.2.2.2 On day 8 at 11:00 UTC, collection of data from Adjacent Regions, States and Organisations is initiated by the Central European DSA. Collection is triggered by schedule or manually by the Central Administrator. In case an Adjacent DSA does not support replication by protocol (DISP), the Central Administrator collects the data by other means (e.g. DSP).

5.4.2.2.3 The Central Administrator validates data provided by Regions, States and Organisations and coordinates with Co-Operating and Adjacent Operators as necessary in order to ensure consistency of data at the last day of the cycle.

5.4.2.2.4 Coordination may take place using any communication means such as email, telephone, fax, etc. At the end of this step, the background area holds a validated set of information.

5.4.2.2.5 The EDS may be complemented by a locking mechanism in case it is considered necessary. Such a locking mechanism would prevent from modifications to the data in the background area during validation and prior to the transfer to pre-operational area.

5.4.2.2.6 On day 14 before 11:00 UTC, the Central Administrator applies workflow and transfers validated data to the pre-operational area of the Managed Data.

5.4.2.2.7 Distribution of Managed Data in the pre-operational area to other Regions, States and Organisations is initiated at 11:00 UTC by the Central European DSA. In case a Co-operating or Adjacent DSA does not support distribution by protocol (DISP), the

respective Operator has to initiate distribution at 11:00 UTC in order to make pre-operational data locally available.

5.4.2.2.8 At the end of this phase, the pre-operational area holds a validated set of information.

5.4.2.3 Acknowledgement Phase

Period:	Phase starts day 15, ends day 20.
Area involved:	None.
Co-operating/Adjacent Operator tasks:	None.
Central Administrator tasks:	None

5.4.2.3.1 No activities are associated with this phase of the EDS Operational Concept.

Note.– This phase is maintained for compatibility with the ATS Messaging Management process in order to allow for implementation of an acknowledgement within the workflow mechanism. Acknowledgement would be required for information generated by the Central European DSA such as routing information.

5.4.2.4 Acknowledgement Processing Phase

Period:	Phase starts day 21, ends day 24.
Area involved:	None
Co-operating/Adjacent Operator tasks:	None
Central Administrator tasks:	None

5.4.2.4.1 No activities are associated with this phase of the EDS Operational Concept.

Note.– This phase is maintained for compatibility with the ATS Messaging Management process in order to allow for implementation of an acknowledgement within the workflow mechanism. Acknowledgement would be required for information generated by the Central European DSA such as routing information.

5.4.2.5 Data Distribution and Implementation Phase

Period:	Phase starts day 25, ends day 28.
Area involved:	Operational
Co-operating/Adjacent Operator tasks:	Initiate distribution if triggered manually. Provide data to legacy applications, i.e. applications without means of access to Directory.
Central Administrator	Make overall data available in operational area.

tasks:	

5.4.2.5.1 The data distribution and implementation phase is used to distribute data in the operational area and to make new data available to operational systems.

5.4.2.5.2 From day 25 on and depending on local policy and needs, data in the pre-operational area is processed by Co-operating and Adjacent Operators. In support of legacy applications without access to Directory services, data in the pre-operational area could be processed for later implementation on the upcoming AIRAC date.

5.4.2.5.3 On day 28 before 11:00 UTC, the Central Administrator applies the workflow and transfers previously validated data from the pre-operational to the operational area of the Managed Data. At 11:00 UTC distribution of Managed Data in the operational area to other Regions, States and Organisations is initiated by the Central European DSA. In case a Co-operating or Adjacent DSA does not support replication by protocol (DISP), the respective Operator has to initiate distribution at 11:00 UTC in order to make operational data locally available.

5.4.2.5.4 At the end of this phase, the operational area holds a new, validated set of information available to the end users. Directory-based and legacy applications make use of the new, validated set of information.

5.5 Authentication and Access Control

5.5.1 Security Policy

5.5.1.1 The EDS Operational Concept defines a security policy for authentication and access control for DSAs and DUAs based on the X.500 standards [9].

5.5.2 Authentication

5.5.2.1 Authentication in the context of Directory services identifies DSAs and Directory users. Authentication for Directory users accessing the Directory through DAP and between DSAs communicating through DSP and DISP is implemented by means of the respective bind and unbind operations of the protocols (Directory Bind/Unbind, DSA Bind/Unbind, DSA Shadow Bind/Unbind). The period of communication is initiated by the bind operation and closed by the unbind operation.

5.5.2.2 Simple authentication is used in the bind operation. Both entities involved shall make use of credentials composed of name and password. Strong authentication would require the establishment of a public key infrastructure and may be used after bilateral agreement between two communication entities.

5.5.3 Access Control

5.5.3.1 Access to the Directory is controlled by granting or denying permissions to perform a particular operation on an element in the DIB. The X.500 security model establishes a framework for the specification of access control which is used to implement access control in the context of the European Directory Service.

5.5.3.2 An access control scheme is associated with every portion of the DIT.

5.5.3.3 The Basic Access Control scheme shall be applied to the DIT. Following the Basic Access Control scheme, the access control decision involves:

- the element being accessed (protected item);
- the user requesting the operation (requestor);
- a right to complete a portion of the operation (permission); and
- one or more attributes governing access to the item (ACI).

5.5.3.4 By means of Basic Access Controls, the EDS Operational Concept establishes access control depending on

- the role of the Directory user,
- the operation performed by the Directory user; and
- the nature and location of the information in the DIB accessed by the Directory user.

5.5.3.5 Section 5.2 identifies the roles as Central Administrator, Co-operating Operator, Adjacent Operator and End User. Chapter 4 categorises the operations as interrogation and modification operations. Access control as given by the EDS Operational Concept distinguishes between interrogation and modification operations The EDS Operational Concept identifies several distinct areas.

5.5.3.6 Access control to the DIB proposed by EDS Operational Concept is summarised as follows, whereas *int* indicates interrogation operations and *mod* indicates modification operations:

Data		**End User**	**Adjacent Operator**	**Co-operating Operator**	**Central Administrator**
Shared	Own	int	int / mod	int / mod	int / mod
	Others	int	int	int	int
Managed	Own Background	-	int / mod	int / mod	int / mod
	Other Background	-	int	int	int
	Pre-operational	-	int	int	int / mod
	Operational	int	int	int	int / mod

Table 2: DIB access control summary

5.6 Cooperation

5.6.1 The EDS Operational Concept focuses on the European Directory Service; however it takes the global role of Directory services into account.

5.6.2 The EDS Operational Concept basically describes the cooperation between the Central European DSA and DSAs implemented by States and Organisations participating in this

concept. The Central European DSA releases Co-operating DSAs from the exchange of information with other participating as well as non-participating States and Organisations.

5.6.3 With respect to non-participating States and Organisations the Central European DSA acts on behalf of participating States and Organisations. All information of participating States and Organisations is exchanged through the Central European DSA.

5.6.4 Overall, the Central European DSA reduces the number of communications relationships for the benefit of participating as well as non-participating Regions, States and Organisations.

6 Schema

6.1 Relationship to Doc 9880 and Community Specification

6.1.1 The schema deployed within the European Directory Service (EDS) implements the schema definition given by ICAO Doc 9880 Part IV [8] and the AMHS CS [1]. This chapter provides the DIT structure and the definition of object classes and attributes types in support of the ATSMHS.

6.2 DIT Structure

6.2.1 In order to allow the EDS to collect, to validate and to distribute data, the DIT definition of the European Directory Service makes use of following DIT structure described in ICAO Doc 9880 Part IV [8].

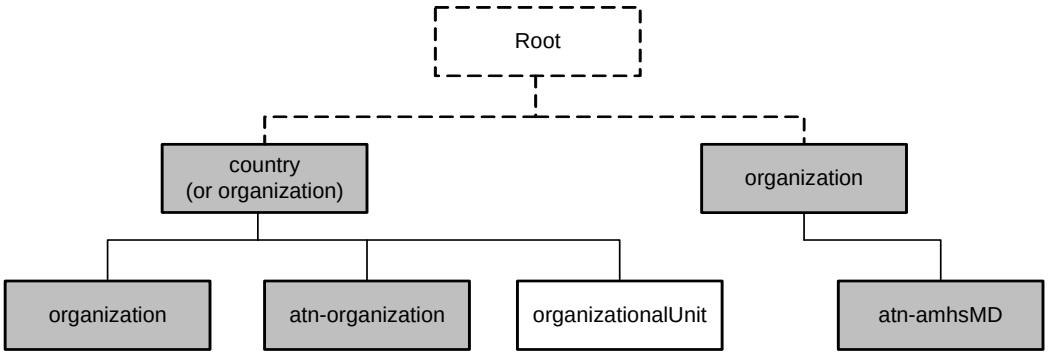

Figure 9: ICAO DIT structure

6.2.2 This addition to the DIT structure given by ICAO Doc 9880 Part IV [8] defines a further element in the DIT below the level of the Organisations that allows the organisation operating the Central European DSA to provide data in a controlled manner. The areas of the Managed Data are represented by the object class organizationalUnit. Depending on the requirements of the applications, the DIT structure below the object class organizationalUnit element may be extended as necessary to hold the information of the respective applications.

6.2.3 The DIT structure in support of the ATSMHS that follows (see Figure 10) includes the elements to hold the information provided by Co-operating and Adjacent States and Organisations as foreseen in section 5.3.5.

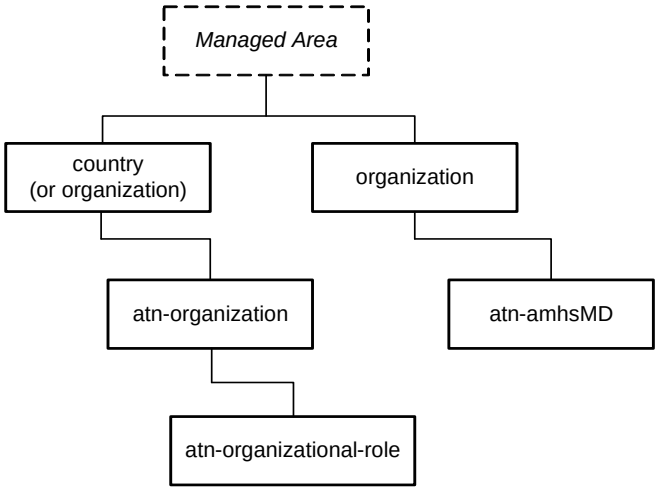

Figure 10: Adapted DIT structure for EDS

6.2.4 The object classes used to hold the AMHS address information have already been outlined in section 5.3.5. The AMHS MD Register is represented by the object class atn-amhsMD allocated below the superior object class organization. The CAAS mapping information is represented by the object class atn-organization allocated below the superior object class country or organization. The user information and the AMHS user capabilities are represented by the object class atn-organizational-role complemented by the auxiliary object class atn-amhs-user allocated below the object class atn-organization.

Note.– The object class atn-amhs-user provides the attribute types for the AMHS user related information, however due to its auxiliary character it is not considered suitable to structure the DIT. The object class atn-organizational-role is used to structure the DIT instead.

6.2.5 Support of further applications is added by extension of the DIT structure as necessary.

6.2.6 In the DIB, the shared data consists of the top-level entries of the States and Organisations as specified by ICAO Doc 9880 Part IV [8] and is replicated from the States and Organisations.

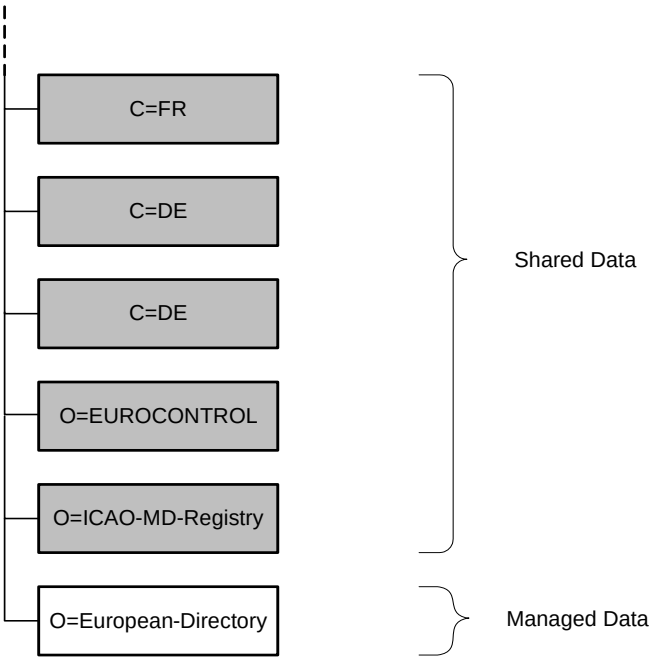

Figure 11: DIT extension for Managed Data

6.2.7 The naming attribute organizationName of the object of class organization representing the Managed Data shall take the value of *European-Directory*.

6.2.8 Within that sub-tree the background, pre-operational and operational areas are represented by entries of object class organizationalUnit. The naming attribute organizationalUnitName shall take the value of the respective area of the Managed Data (*Background*, *Pre-operational*, *Operational*).

6.2.9 Managed Data is subject to workflow mechanisms and supports different sets of data (versions). Different versions of data are stored in different sub-trees of the DIT.

6.2.10 The value of the attribute description of the object class organizationalUnit indicates the respective AIRAC cycle as specified by the ATS Messaging Management Manual [3].

6.2.11 The following example gives the situation for operational cycle 102, whereas information for cycle 103 is already available in the background and pre-operational areas.

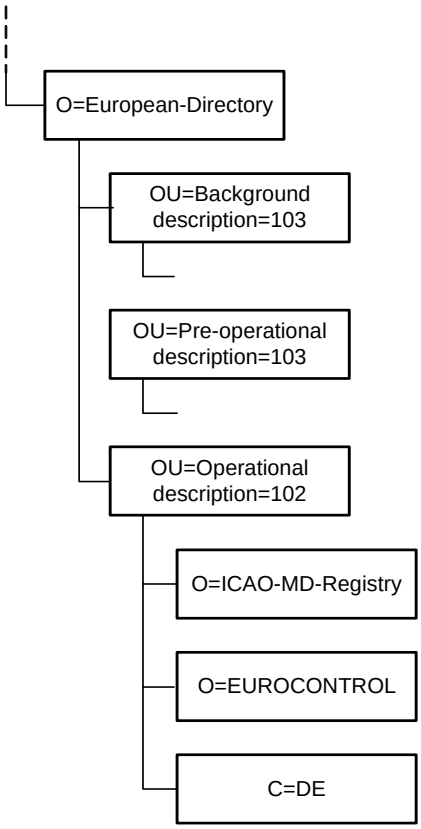

Figure 12: Example of information for operational cycle 102 and cycle 103

6.2.12 The data in the DIB of the EDS will initially be based on data currently maintained in the AMC. Section 5.3.5 lists the tables in AMC and their respective object classes in the EDS.

6.2.13 The following sections describe the additional object classes and attribute types used to structure the DIT and to hold this data.

6.3 Object Classes

6.3.1 Basic object classes

6.3.1.1 ISO/IEC 9594-7, a standard of the X.500 series [10], contains a number of basic object classes. The definition of the ATN-specific object classes in ICAO Doc 9880 Part IV [8] refers to these basic object classes.

6.3.1.2 In EDS the following MHS object class is used:

```
mhs-distribution-list   OBJECT-CLASS ::= {
        SUBCLASS OF         { top }
        MUST CONTAIN        { commonName |
                              mhs-dl-submit-permissions |
                              mhs-or-addresses }
        MAY CONTAIN         { description |
                              organizationName |
                              organizationalUnitName |
                              owner |
                              seeAlso |
```

```
                                    mhs-maximum-content-length |
                                    mhs-deliverable-content-types |
                                    mhs-acceptable-eits |
                                    mhs-exclusively-acceptable-eits |
                                    mhs-unacceptable-eits |
                                    mhs-dl-policy |
                                    mhs-dl-subscription-service |
                                    mhs-dl-archive-service |
                                    mhs-dl-related-lists |
                                    mhs-dl-members }
                                    ID      id-oc-mhs-distribution-list }
```

- with MHS attribute type:

```
mhs-dl-submit-permissions   ATTRIBUTE ::= {
                WITH SYNTAX         DLSubmitPermission
                ID                  id-at-mhs-dl-submit-permissions }
```

- with MHS syntaxes:

```
ContentLength ::= INTEGER (0..ub-content-length)

DLSubmitPermission ::= CHOICE {
        Individual          [0]     ORName,
        member-of-dl        [1]     ORName,
        pattern-match       [2]     ORNamePattern,
        member-of-group     [3]     Name}
```

6.3.2 ATN-specific object classes

6.3.2.1 This section lists the ATN-specific object classes in support of the ATSMHS.

6.3.2.2 The ATN-specific object class ***atn-organization*** shall be defined by the ASN.1 syntax:

```
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 }
```

6.3.2.3 The ATN-specific object class ***atn-amhsMD*** shall be defined by the ASN.1 syntax:

```
atn-amhsMD MD 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 }
```

6.3.2.4 The ATN-specific object class ***atn-organizational-role*** shall be defined by the ASN.1 syntax:

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

6.3.2.5 The ATN-specific object class ***atn-amhs-user*** shall be defined by the ASN.1 syntax:

```
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 |
                          atn-maximum-number-of-body-parts |
                          atn-maximum-text-size |
                          atn-maximum-file-size |
                          mhs-message-store-dn |
                          atn-per-certificate |
                          atn-der-certificate |
                          atn-use-of-amhs-security |
                          atn-use-of-directory |
                          atn-group-of-addresses |
                          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.

6.3.2.6 The ATN-specific object class ***atn-amhs-distribution-list*** shall be defined by the ASN.1 syntax:

```
atn-amhs-distribution-list OBJECT-CLASS ::= {
        SUBCLASS OF     { mhs-distribution-list }
        MUST CONTAIN    { atn-ipm-heading-extensions }
        MAY CONTAIN     { atn-maximum-number-of-body-parts |
                          atn-maximum-text-size |
                          atn-maximum-file-size |
                          atn-per-certificate |
                          atn-der-certificate |
                          atn-use-of-amhs-security |
                          atn-use-of-directory |
                          atn-AF-address }
        ID              id-oc-atn-AmhsDistributionList }
```

6.4 Attribute Types

6.4.1 Basic attributes types

6.4.1.1 ISO/IEC 9594-6, a standard of the X.500 series [10], contains a number of basic attributes types. The definition of the ATN-specific attribute types in ICAO Doc 9880 Part IV [8] refers to these basic attribute types.

6.4.2 ATN-specific attribute types

6.4.2.1 This section lists the ATN-specific attribute types in support of the ATSMHS.

6.4.2.2 The ATN-specific attribute ***atn-facility-name*** shall be defined by the ASN.1 syntax:

```
atn-facility-name ATTRIBUTE ::= {
        WITH SYNTAX     PrintableString(SIZE(1..64))
        ID              id-at-atn-facilityName }
```

6.4.2.3 The ATN-specific attribute ***atn-global-domain-identifier*** shall be defined by the ASN.1 syntax:

```
atn-global-domain-identifier ATTRIBUTE ::= {
        WITH SYNTAX     mhs-or-address
        SINGLE VALUE    TRUE
        ID              id-at-atn-amhs-global-domain-identifier }
```

6.4.2.4 The ATN-specific attribute ***atn-icao-designator*** shall be defined by the ASN.1 syntax:

```
atn-icao-designator ATTRIBUTE ::= {
        WITH SYNTAX     PrintableString(SIZE(2..7))
        ID              id-at-atn-icao-designator }
```

6.4.2.5 The ATN-specific attribute ***atn-amhs-addressing-scheme*** shall be defined by the ASN.1 syntax:

```
atn-amhs-addressing-scheme ATTRIBUTE ::= {
        WITH SYNTAX     INTEGER {
                            xf (0),
                            caas (1),
                            other (2)}
        SINGLE VALUE    TRUE
        ID              id-at-atn-Amhs-addressing-scheme }
```

6.4.2.6 The ATN-specific attribute ***atn-amhsMD-naming-context*** shall be defined by the ASN.1 syntax:

```
atn-amhsMD-naming-context ATTRIBUTE ::= {
        WITH SYNTAX     PrintableString(SIZE(1..64))
        SINGLE VALUE    TRUE
        ID              id-at-atn-AmhsMD-naming-context }
```

6.4.2.7 The ATN-specific attribute ***atn-ipm-heading-extensions*** shall be defined by the ASN.1 syntax:

```
atn-ipm-heading-extensions ATTRIBUTE ::= {
        WITH SYNTAX     BOOLEAN
        ID              id-at-atn-ipm-heading-extensions }
```

6.4.2.8 The ATN-specific attribute ***atn-amhs-direct-access*** shall be defined by the ASN.1 syntax:

```
atn-amhs-direct-access ATTRIBUTE ::= {
        WITH SYNTAX     BOOLEAN
        ID              id-at-atn-amhs-direct-access }
```

6.4.2.9 The ATN-specific attribute ***atn-per-certificate*** shall be defined by the ASN-1 syntax:

```
atn-per-certificate ATTRIBUTE ::= {
        WITH SYNTAX     OCTET STRING
        ID              id-at-atn-PerCertificate }
```

6.4.2.10 The ATN-specific attribute ***atn-der-certificate*** shall be defined by the ASN-1 syntax:

```
atn-der-certificate ATTRIBUTE ::= {
        WITH SYNTAX     Certificate
        ID              id-at-atn-DerCertificate }
```

6.4.2.11 The ATN-specific attribute ***atn-AF-address*** shall be defined by the ASN.1 syntax:

```
atn-AF-address ATTRIBUTE ::= {
        WITH SYNTAX     PrintableString (SIZE(8))
        SINGLE VALUE    TRUE
        ID              id-at-atn-AF-address }
```

6.4.2.12 The ATN-specific attribute ***atn-maximum-number-of-body-parts*** shall be defined by the ASN.1 syntax:

```
atn-maximum-number-of-body-parts ATTRIBUTE ::= {
        WITH SYNTAX     INTEGER
        SINGLE VALUE    TRUE
        ID              id-at-atn-maximum-number-of-body-parts }
```

6.4.2.13 The ATN-specific attribute ***atn-maximum-text-size*** shall be defined by the ASN.1 syntax:

```
atn-maximum-text-size ATTRIBUTE ::= {
        WITH SYNTAX     ContentLength
        SINGLE VALUE    TRUE
        ID              id-at-atn-maximum-text-size }
```

6.4.2.14 The ATN-specific attribute ***atn-maximum-file-size*** shall be defined by the ASN.1 syntax:

```
atn-maximum-file-size ATTRIBUTE ::= {
        WITH SYNTAX     ContentLength
        SINGLE VALUE    TRUE
        ID              id-at-atn-maximum-file-size }
```

6.4.2.15 The ATN-specific attribute ***atn-use-of-amhs-security*** shall be defined by the ASN.1 syntax:

```
atn-use-of-amhs-security ATTRIBUTE ::= {
        WITH SYNTAX         BOOLEAN
        SINGLE VALUE        TRUE
        ID                  id-at-atn-use-of-amhs-security }
```

6.4.2.16 The ATN-specific attribute ***atn-use-of-directory*** shall be defined by the ASN.1 syntax:

```
atn-use-of-directory ATTRIBUTE ::= {
        WITH SYNTAX         BOOLEAN
        SINGLE VALUE        TRUE
        ID                  id-at-atn-use-of-directory }
```

6.4.2.17 The ATN-specific attribute ***atn-group-of-addresses*** shall be defined by the ASN.1 syntax:

```
atn-group-of-addresses ATTRIBUTE ::= {
        WITH SYNTAX         BOOLEAN
        SINGLE VALUE        TRUE
        ID                  id-at-atn-group-of-addresses }
```

7 Transition

7.1 General Considerations

7.1.1 Seamless operation of ATN applications needs to be ensured during the transition from current environment to European Directory Service (EDS).

7.1.2 Additional means are essential to allow for a smooth introduction of the European Directory Service and to assure continuous operation of ATN applications using other methods of data management.

7.2 Deployment of EDS

7.2.1 Starting point

7.2.1.1 The EDS Operational Concept adopts, for the Managed Data, the AIRAC cycle including duration and phases as specified by the ATS Messaging Management Manual [3] to limit changes in existing procedures and to ease transition. Since the Central European DSA creates or modifies no data, no activities are associated with the Acknowledgement and Acknowledgement Processing Phases. The initial duration of a cycle for Managed Data is aligned to the ATS Messaging Manual process and takes 28 days. Given the fact that no activities are associated with the Acknowledgement and Acknowledgement Processing Phases it may be possible to reduce the duration to take less than 28 days if considered necessary at a later stage.

7.2.1.2 At the time of development of the EDS Operational Concept some of the information intended to be held by the European Directory Service is managed and distributed using the ATS Messaging Management Centre (AMC). Within the AMHS address management, the AMC maintains the AMHS MD Register, CAAS tables and user address lookup tables. The management and distribution of AMHS addresses through AMC is provided by EUROCONTROL on behalf of ICAO Headquarters as published by State Letter in April 2009. Furthermore the AMC implements AMHS user capabilities management. The AMC provides exports of this information available in comma separated value (CSV).

7.2.1.3 It is proposed to transfer management and distribution of this information in three steps to the European Directory Service. The required object classes and attribute types have been identified in section 5.3.5.

7.2.2 Initial Step

7.2.2.1 In the first, initial step the information is still maintained and stored using the AMC.

7.2.2.2 The AMC is the single, authoritative source of the information. In addition to the AMC export functions, the information is made available by the European Directory Service. Depending on local requirements States and Organisations decide on the services to be used.

7.2.2.3 The AMC provides information to the Central European DSA either by online or offline means. The European Directory Service is used for distribution of information, but not for collection and management. No workflow mechanism is implemented by the Central European DSA, since this task is still performed by the AMC. With respect to the description

of procedures in section 5.4, only phases 3 (acknowledgment) and 5 (data distribution and implementation) are implemented by the EDS. In the acknowledgment phase, data is made available in the pre-operational area. In the data distribution and implementation phase, data is made available in the operational area.

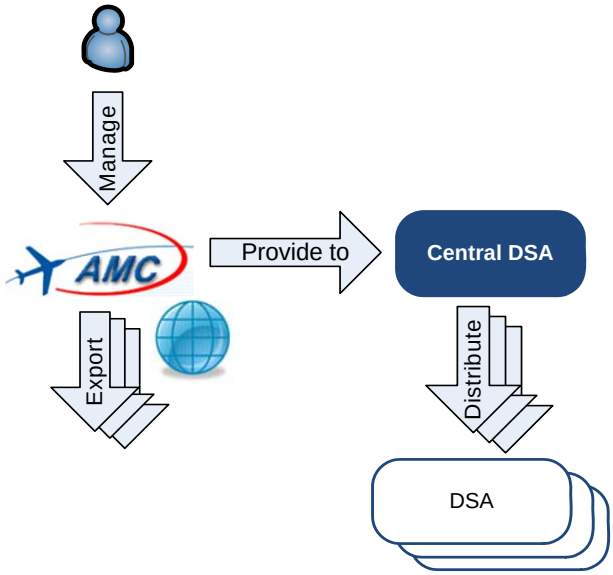

Figure 13: Interaction AMC – EDS (Initial step)

7.2.2.4 In this step the AMC still performs all known functions. The European Directory Service distributes information in addition to distribution means provided by the AMC. No transitional aids are required in this step since the range of AMC functions is fully maintained in this step.

7.2.3 Intermediate Step

7.2.3.1 In the intermediate step, storage of relevant information currently held by the AMC database is moved from AMC to the European Directory Service. At this stage depending on the requirements of the users the EDS might include additional data besides the information held in AMC. The Directory becomes the single, authoritative source of information. The AMC is equipped with an Administrative DUA in order to allow AMC users to view and manage information, which is now stored in the Directory. The Central European DSA implements the workflow mechanism as given by the ATS Messaging Management Manual.

7.2.3.2 The AMC and EDS are available in parallel. States and Organisations decide whether they use AMC or Directory services for management of information depending on their needs and availability of local Directory services. When the AMC is used for management of information, it will access the Central European DSA through the built-in Administrative DUA, in order to perform interrogation and modification operations. AMC exports and distribution of information by the European Directory Service could be used simultaneously serving different needs of applications. With respect to the description of procedures in section 5.4, all phases are now implemented by the EDS.

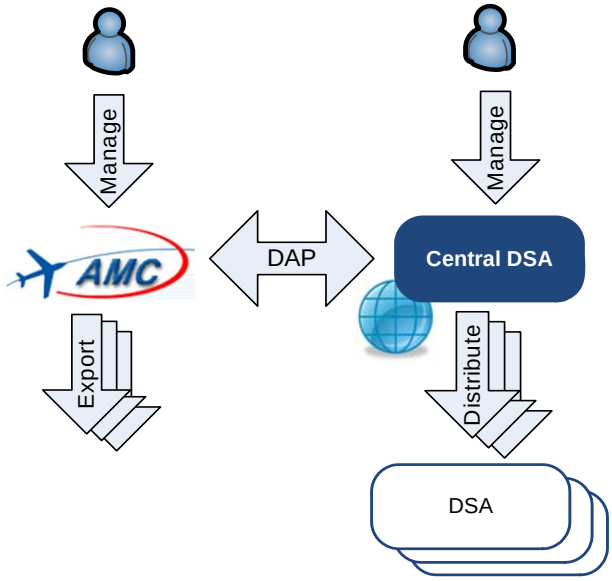

Figure 14: Interaction AMC – EDS (Intermediate step)

7.2.3.3 Implementation of the intermediate step is transparent to end users and has no impact to systems using the information. In this step, AMC workflow is transferred to the Central European DSA. However the AMC export functions are available in addition to distribution of information by the European Directory Service. Transitional aids might be provided in order support migration from AMC to European Directory Service. Details on transitional aids are provided in section 7.3.

7.2.4 Final Step

7.2.4.1 In the final step the AMHS common functions now reside within EDS and thus are disabled in the AMC. The AMC no longer accesses the European Directory Service.

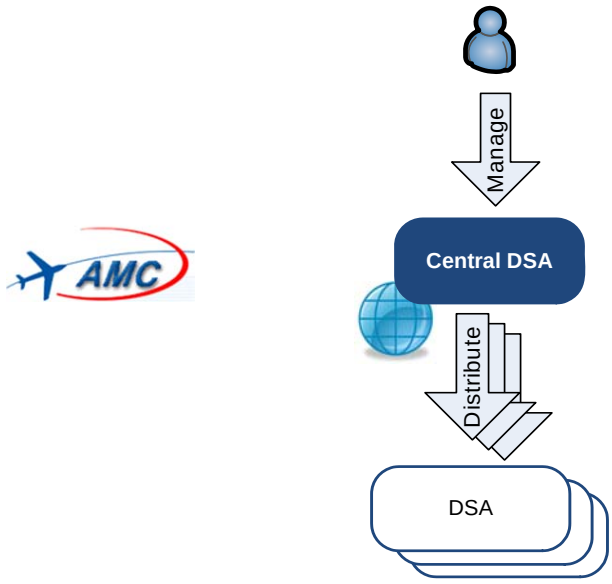

Figure 15: Interaction AMC – EDS (Final step)

7.2.4.2 In the beginning of the final step some States and Organisations might not implement Directory services and might not contribute to the overall function of Directory services. Transitional aids as outlined below are essential means for States and Organisations who do not participate in Directory services and operate legacy applications without means to access the European Directory Service.

7.3 Transitional Aids and Aspects

7.3.1 Need of Transitional Aids

7.3.1.1 Transitional aids may be required by States and Organisations which have not yet implemented Directory services or are operating legacy application without access to Directory services by protocol. Several means are available in support of transition to Directory services. During step 1 (initial) and step 2 (intermediate) transitional aids could be useful to support early introduction of Directory services at the local level. Those transitional aids become essential in step 3 (final) when AMC no longer provides management and distribution of AMHS address information.

7.3.1.2 Deployment of Operational Personnel DUAs and provision of web access to the European Directory Service could provide appropriate means to serve Directory data to End Users without a local implementation of Directory services. Future Co-operating or Adjacent Operators may be equipped with an Administrative DUA to allow for management of data. Deviating from the policy given in this document, these users may, by means of their DUAs, directly access the Central European DSA for the purpose of data management and retrieval of information. Direct access of Autonomous Operational DUAs to the European Directory Service is strongly discouraged.

7.3.2 Administrative DUA

7.3.2.1 In the case where a State or Organisation does not participate in European Directory Service through a Co-operating or Adjacent DSA, but has already implemented an

administrative DUA, the Central European DSA grants direct access to Managed Data at the Central European DSA for the purpose of data management using that DUA.

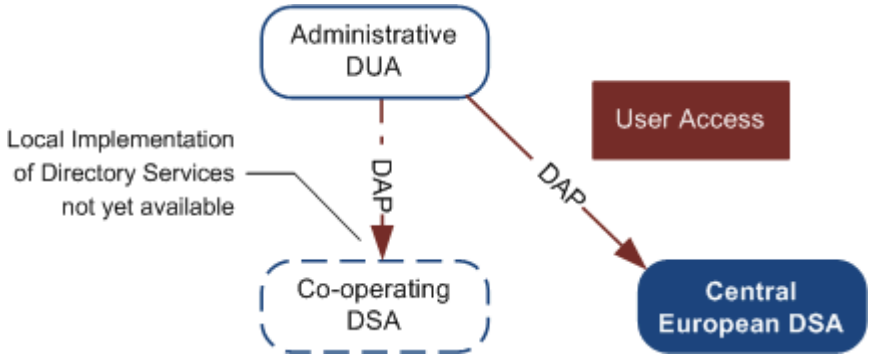

Figure 16: Direct access of DUA to Managed Data via DAP

7.3.2.2 Furthermore, the Central European Directory Service might supply administrative DUAs to States and Organisations without local Directory infrastructure. This would allow States and Organisations to manage their data at the Central European DSA prior to implementation of local Directory services and full participation in the European Directory Service.

7.3.3 Operational Personnel DUA

7.3.3.1 In the case where a State or Organisation does not participate in the European Directory Service through a Co-operating or Adjacent DSA, but has already implemented an Operational Personnel DUA, the Central European DSA grants – similar to the situation above – direct access to Managed Data at the Central European DSA for the purpose of data retrieval using that DUA.

7.3.3.2 Using an Operational Personnel DUA, the Lightweight Directory Access Protocol (LDAP) Data Interchange Format (LDIF) [12] might be used to export data from European Directory Service and to provide legacy systems without the capability to make use of Directory with required information.

7.3.3.3 Furthermore, the European Directory Service might supply Operational Personnel DUAs to States and Organisations without local Directory infrastructure. This would allow States and Organisations to retrieve data from the Central European DSA prior to implementation of local Directory services.

7.3.4 Web Access

7.3.4.1 In addition, the Central European DSA might be enhanced by web access that allows users representing future Co-operating or Adjacent Operators to access data at the Central European DSA. Web access would make use of wide-spread Internet technology. On the back-end the web access will have to implement an Administrative DUA using DAP for access to the Central European DSA. Such a web service would have to provide an authentication and authorisation mechanism in order to establish a high level of security and to assign appropriate access rights to the user accessing the EDS at the Central European DSA.

7.3.4.2 In the case where the Central European DSA implements web access as a transitional means, States and Organisations not participating in Directory services can manage their data and access other data at the Central European DSA through the web interface.

7.3.4.3 During transition, the Central European DSA might supply Adjacent DSAs with data regarding other Adjacent DSAs.

7.3.4.4 The introduction of the European Directory Service would significantly benefit from an existing European IP-based network infrastructure that connects the sites of Co-operating States and Organisations with the site of the Central European DSA. For the exchange of information with Adjacent DSAs, the Central European DSA depends on international network connectivity.

8 Capacity and Performance Considerations

8.1 This chapter discusses capacity and performance considerations with respect to the implementation of the centralised European Directory Service (EDS).

8.2 In a fully distributed environment as anticipated by ICAO documentation there might be overall more than 200 communication partners in the ATN Directory service, about 50 of which belong to the European area. Such a large number of communication partners per entity would cause significant issues in configuration, management and operation for each individual DSA participating in ATN Directory services.

8.3 The implementation of a centralised European Directory Service would considerably reduce the number of communication relationships per entity. However, for Regions, States and Organisations not participating in the concept, but implementing an Adjacent DSA, the Central European DSA acts on behalf of Co-operating States and Organisations.

8.4 Instead of up to about 50 individual communication relationships to every Co-operating State and Organisation, Adjacent DSAs have to establish and maintain exactly one communication relationship to the Central European DSA. For Co-operating DSAs the advantage is even more obvious. Instead of communication relationships to every other DSA, which can sum up to over 200, Co-Operating DSAs have to establish and maintain exactly one communication relationship to the Central European DSA.

8.5 Centralised European Directory Service scales very well with regard to increase of Co-Operating States and Organisations. The increase of Adjacent DSAs remains widely transparent to Co-Operating States and Organisations.

8.6 Besides the advantages at the level of applications, the implementation of centralised European Directory Service would also have a positive impact to networking requirements reducing the need to establish an international fully meshed network.

8.7 The implementation of centralised Directory services with critical information being replicated periodically to other DSAs, reduces the need for a fast, high-performance underlying network. The quality of service requirements are lower compared to distributed environments; especially with regard to bandwidth and latency.

8.8 In a distributed environment every DSA would only hold the information related to the State or Organisation operating that DSA. For information related to other Regions, States, or Organisations the respective DSA of that Region, State or Organisation has to provide the information. With a centralised, replicated topology, all relevant information is replicated and locally available. The amount of information stored per DSA is higher in replicated environments; however this is not expected to cause capacity issues.

9 Future Options

9.1 This chapter outlines future options of the European Directory Service (EDS).

9.2 ICAO Doc 9880 Part I [5] already identifies some more ATN applications to make use of Directory services such the Context Management (CM) application. By means of the CM registration functions further ATN application such as the Controller-Pilot Data Link (CPDLC) application make indirect use of Directory services.

9.3 The EDS Operational Concept takes into account the requirements to support the ATSMHS, but is not limited to the ATSMHS or ground-ground applications in general. ICAO Doc 9880 Part IV [8] already defines additional ATN-specific attribute types and object classes beyond the scope of AMHS such as the object class atn-aircraft.

9.4 Security is a global field of interest with growing relevance to existing and future applications. The AMHS CS [1] already includes AMHS Security as an informative element as it was not yet considered as advanced as other elements of the Extended ATS Message Handling Service (ATSMHS). AMHS Security and security services in general are expected to be based on the establishment and use of a Public Key Infrastructure (PKI). Using certificates issued by certification authorities (CAs) enables protection against a multitude of threats such as masquerade, modification, replay, etc. To this end, ICAO Doc 9880 Part IV [8] defines the essential standard attributes types and mandatory objects classes, including, where relevant, attribute types to hold certificates in ATN-specific object classes.

9.5 The generic nature and openness of X.500 Directory services, which forms the base of the European Directory Service, facilitates support of future requirements to further extend the schema (attribute types, object classes, etc.), to increase the amount of data and to expand the service to other applications as necessary.

9.6 As an example, in case a global information management system, such as the System Wide Information Management (SWIM) currently under development, implements tailored authentication and authorisation in order to manage access to distributed data, the schema definition of the European Directory Service could be expanded to meet its needs. Such an expansion could include the specification of additional application-specific attribute types and objects classes and the expansion of the Directory Information Tree in order to hold the respective data.

9.7 Even though the basic schema definition needs to be shared between all involved DSAs and DUAs, the X.500 Directory standards also allows for regional, national and organisational extensions that are not shared on a global basis. Such extensions would allow to satisfy local needs and to implement dedicated added value services such as white pages, address books, registers, etc.

9.8 With the specification of the centralised European Directory Service that also covers centralised management of data including a workflow mechanism, the EDS Operational Concept describes a way of how data can be collected, validated and distributed in a controlled way. The centralised management of data is given in a universal and generic way, which allows its use whenever considered useful.

- END of Appendix G -