EUR AMHS Manual

Appendix G-A

EDS User Interface Control Document	
Document Reference:	EUR AMHS Manual, Appendix G-A
Author:	EUROCONTROL, Planning Group
Revision Number:	Version 16.0
Date:	20/10/2021
Filename:	EUR_AMHS_Manual-Appx_G-A_v16_0.doc

Document Control Log

Edition	Date	Comments	section/pages affected
0.1	13/01/2016	Creation of the document based on EUROCONTROL document [9]	all
0.2	17/02/2017	Editorial modifications Inclusion of material concerning Guidance for Modifications of the DirectorySchema	all
1.0	04/04/2017	Final version for presentation to AFSG/21 as attachment to CP-AMHSM-16-001 and CP-AMHSM-16-006	all
12.0	28/04/2017	Adopted version (AFSG/21)	
12.1	23/04/2018	Incorporation of CP-AMHSM-17-004	References
13.0	27/04/2018	Adopted version (AFSG/22)	
13.1	11/02/2019	Incorporation of CP-AMHSM-18-001	4.1.15, 4.1.16, 4.1.17, 4.1.18 4.2.9, 5.1.3
14.0	05/03/2019	Adopted version (AFSG/23)	
14.1	26/11/2019	Incorporation of CP-AMHS-19-002 Adaption: According to COG/74&RCOG/11 Decision /4, Approval of AFS to SWIM Transition Task Force (AST TF) Terms of Reference (ToR) and coherent Work Programme, the Author of EUR Doc 020 changed from “AFSG PG” to “AST PG”.	all
15.0	12/11/2020	Adopted version (AST TF/01)	
16.0	20/10/2021	Adopted version (AST TF/02)	

Table of contents

References

[1] ICAO Annex 10 – Aeronautical Telecommunications, Volume II: Communication Procedures, Seventh Edition, July 2016

[2] 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), 2nd Edition, 2016

[3] 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 Identifier Registration, 2nd Edition, 2016

[4] ICAO Doc 9896 Manual on the Aeronautical Telecommunication Network (ATN) using Internet Protocol Suite (IPS) Standards and Protocol, 2nd Edition, 2015

[5] EUR Doc 020, EUR AMHS Manual

[6] EUR Doc 021, ATS Messaging Management Manual,

[7] 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.

[8] EUROCONTROL European Directory Service (EDS) – Operational Concept – WP2 (Concept), Version 1.0, 26/10/2011

[9] EUROCONTROL European Directory Service – EDS User Interface Manual – Version 2.0 Edition Date: 11/12/2015, Status: Released Issue, Intended for: AFSG

[10] ISO/IEC 7498-1 Information technology – Open Systems Interconnection – Basic Ref. Model: The Basic Model, 2nd Edition, 1994

[11] 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.

[12] ISO/IEC 10021-7 Information technology – Message Handling Systems (MHS) – Interpersonal Messaging System, 2003

[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

Table of Figures

List of Tables

1 Introduction

1.1 Scope of the Document

1.1.1 This document describes the interface of European Directory Service (EDS) for co-operating and adjacent users. It summarises interface details for the exchange of information between the Central European DSA, and Co-operating and Adjacent DSAs.

1.1.2 The European Directory Service (EDS) is the implementation of ATN Directory services [3] 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.

1.1.3 EUROCONTROL has implemented the Central European DSA for the initial step according to the EDS Operational Concept initially defined in the EUROCONTROL EDS Operational Concept document [8], adopted by the Aeronautical Fixed Services Group (AFSG) and published in Appendix G to ICAO EUR Doc 020 (EUR AMHS Manual) [5].

1.1.4 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 Co-operating and Adjacent DSAs.

1.2 Purpose of the Document

1.2.1 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 DSAs on the other hand. The document summarises the communications means of EDS. It shall assist in setting up communications with the Central European DSA. Furthermore, it includes guidance material and advice for trouble shooting.

1.2.2 The operators, engineering and maintenance personnel of States or Organisations operating Co-operating and Adjacent DSAs are the intended, primary audience of this document. In addition, this document might serve implementers and users as guidance material.

1.3 Structure of the Document

1.3.1 This document is composed of the following chapters:

- Chapter 1 (this chapter) contains an introduction to the document.
- Chapter 2 gives an overview on EDS and the EDS user interface.
- Chapter 3 specifies the EDS interface protocols.
- Chapter 4 provides guidance on setup of systems.
- Chapter 5 gives assistance for trouble-shooting.
- Chapter 6 provides guidelines for software updates and directory structure changes.

2 Overview

2.1 EDS Operational Concept

2.1.1 The EDS Operational Concept adopts and refines the approach given by the AMHS Community Specification [7], further referred to as AMHS CS. The AMHS CS (Chapter 4) outlines a centralised Directory service as a European Common Facility.

2.1.2 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 European DSA and/or States and Organisations participating in the concept.

2.1.3 The EDS Operational Concept given in Appendix G to ICAO EUR Doc 020 (EUR AMHS Manual) [5] 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.

2.2 Topology

2.2.1 The EDS Operational Concept describes an overall online Directory solution. In the framework of the European Directory Service (EDS) 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. 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.

2.2.2 The EDS Operational Concept as specified in Appendix G to ICAO EUR Doc 020 (EUR AMHS Manual) [5] describes the relationship of the Central European DSA with Co-operating and Adjacent DSAs implemented by participating and non-participating States and Organisations. Figure 1 gives an abstract overview of the EDS topology.

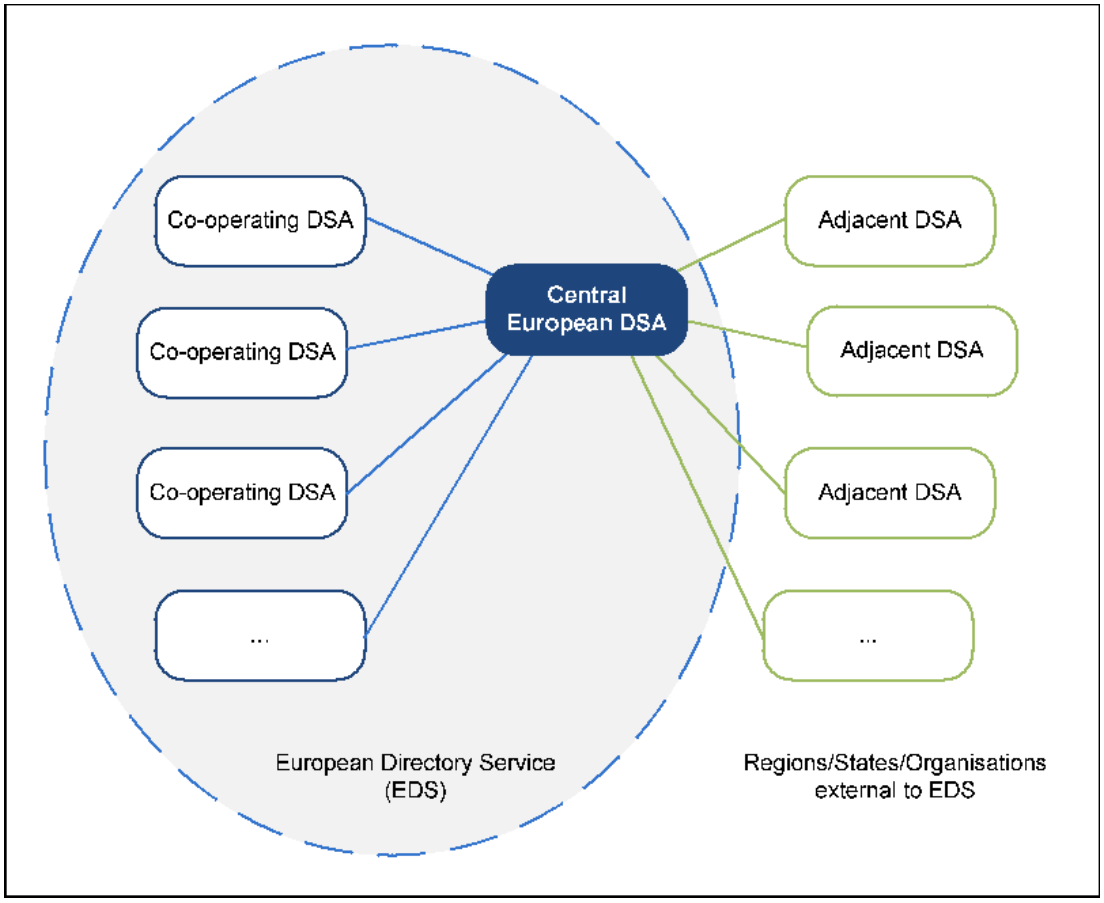

Figure 1: EDS Topology

2.3 Flow of Information – Initial Step

2.3.1 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.

2.3.2 In line with the procedures specified in ICAO EUR Doc 021 (ATS Messaging Management Manual) [6], 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 when:

- Pre-operational Area status becomes ‘in preparation’ or ‘proposed’;
- Pre-operational Area status becomes ‘released’; and
- Pre-operational Area with status ‘released’ is moved to the Operational Area

2.3.3 The basic flow of information in the initial step of the EDS Operational Concept as specified by the EUR AMHS Manual [5] is outlined in Figure 2 below.

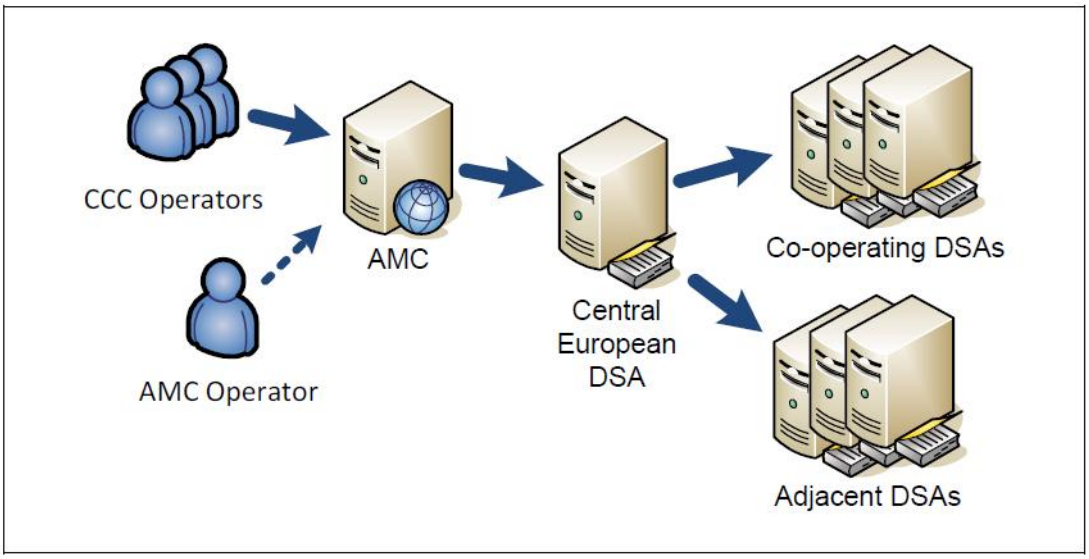

Figure 2: Flow of Information – Initial step

2.3.4 The processing of the information provided at the Co-operating and Adjacent DSAs by the Central European DSA and the provision of information to end users is a local matter and considered out of scope.

2.4 EDS User Interface

2.4.1 The focus of this document is the EDS user interface between the Central European DSA and the EDS users, as outlined in Figure 3. In this context, EDS users are identified as the users of the centralised service provided by the Central European DSA, as a European 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.

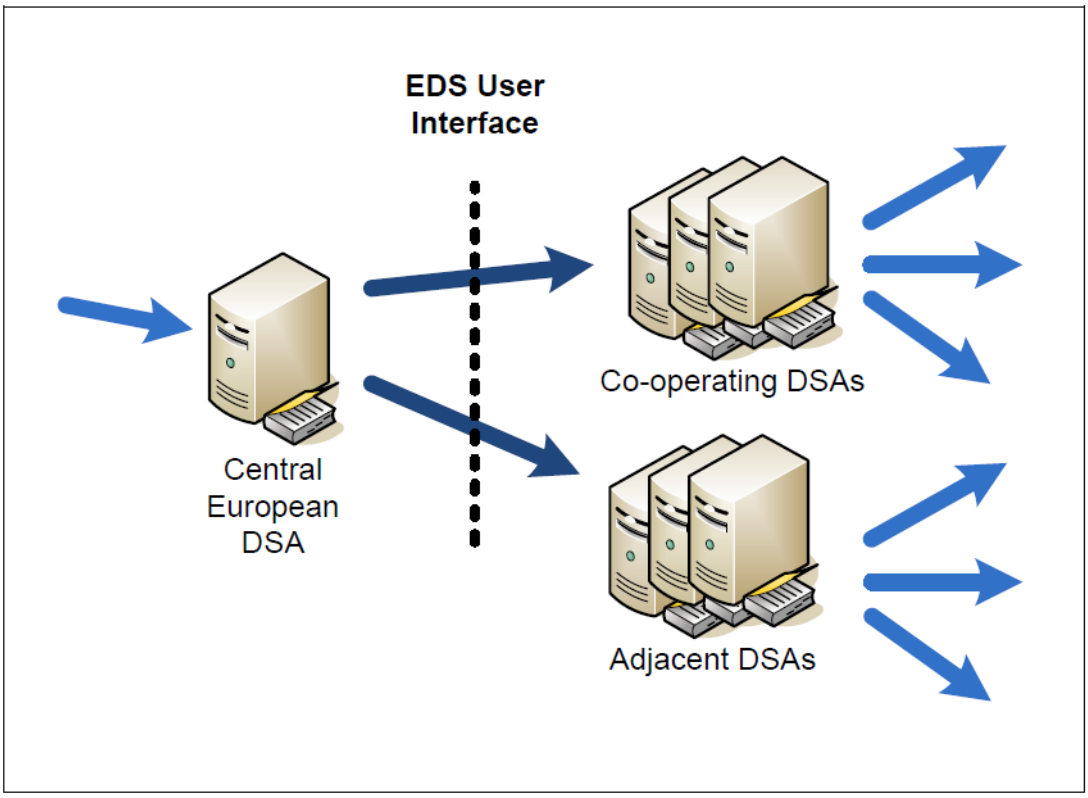

Figure 3: EDS User Interface

3 EDS Interface Protocols

3.1 General

3.1.1 This chapter recaps the X.500 protocols deployed between the Central European DSA, and Co-operating and Adjacent DSAs, further referred to as peer DSAs.

3.1.2 The EDS Operational Concept identifies the Directory Information Shadowing Protocol (DISP) and the Directory System Protocol (DSP) for exchange of information between peer DSAs.

3.2 Directory Information Shadowing Protocol

3.2.1 The Directory Information Shadowing Protocol (DISP) specified in ISO/IEC 9594-9 [11] 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 [7], the EDS Operational Concept recommends DISP for the purpose of distribution of information from the Central European DSA to Co-operating and Adjacent DSAs.

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

3.2.3 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-operating 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. Prior to perform shadowing, the Central European DSA establishes an application association as necessary using the operation *dSAShadowBind* which corresponds to the operation *dSABind*, if not already established as a result of a previous action. Shadowing is performed through the shadowing operations *coordinateShadowUpdate* and *updateShadow*.

3.3 Directory System Protocol

3.3.1 The Directory System Protocol (DSP) specified in ISO/IEC 9594-5 [11] supports communications between two DSAs, where a request for information cannot or at least cannot fully be resolved by one DSA and is forwarded to another DSA.

3.3.2 Taking into account available products, implementations and the fact that DISP was not mandated by ICAO Doc 9880 Part IV [3] or the AMHS CS [7], the EDS Operational Concept allows for other, non-standard or proprietary means of bulk retrieval from the Central European DSA using chaining by DSP.

3.3.3 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 c*hainedread* and c*hainedlist*. Bulk retrieval needs to be initiated by a specialised Directory

User Agent (DUA), which 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 or Adjacent DSA establishes an application association by means of the operation *dSABind*, if not already established as a result of a previous action.

3.3.4 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 Setup of the EDS Systems

4.1 Prerequisites

4.1.1 This section establishes basic conformance requirements that are considered prerequisites for interoperability and validation testing.

4.1.2 A Co-operating or Adjacent DSA is an implementation of an X.500 Directory System Agent (DSA). Co-operating and Adjacent DSA have to implement the profiles identified by ICAO Doc 9880 Part IV [3] and the AMHS Community Specification [7]. Support of DISP is strongly recommended, however not mandated.

4.1.3 *Conformance Requirement:* An implementation of a Co-operating or Adjacent DSA shall conform to ISO/IEC 9594 set of standards [11] and the profiles defined by ICAO Doc 9880 Part IV [3] and the AMHS Community Specification [7].

4.1.4 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 [10]. In case DISP is not supported by an implementation, distribution of information could be achieved through DSP requiring some additional effort for the development of a specialised DUA implementing pull distribution.

4.1.5 *Conformance Requirement:* The implementation of the Directory Information Shadowing Protocol (DISP) by a Co-operating or Adjacent DSA shall conform to ISO/IEC 9594-9 [11] supporting simple authentication and on-change, supplier-initiated, total and incremental updates.

4.1.6 *Conformance Requirement:* The implementation of the Directory System Protocol (DSP) by a Co-operating or Adjacent DSA shall conform to the ISO/IEC 9594-5 [11] supporting simple authentication and chaining of type cross reference.

4.1.7 EDS follows the principles of IP-based networking set out in the ICAO Doc 9896 [4] and ICAO EUR Doc 020 (EUR AMHS Manual) [5]. 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 [13]. In support of future use of the Internet Protocol version 6 (IPv6), provisions for an ISO transport mapping on top of TCP according to RFC 2126 [14] is recommended.

4.1.8 *Conformance Requirement:* A Co-operating or Adjacent DSA shall implement the ISO transport service on top of TCP (transport mapping) in conformance with RFC 1006 [13] for IPv4. In case the implementation supports IPv6, the implementation of the transport mapping shall conform to RFC 2126 [14].

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

4.1.9 The Directory schema of EDS is defined in Appendix G-B to ICAO EUR Doc 020 (EUR AMHS Manual) [5]. The implementation needs to support the relevant basic, the ATN-specific and the EDS-specific attribute types and object classes.

4.1.10 *Conformance Requirement:* The Directory schema implemented by Co-operating and Adjacent DSAs shall conform to the EDS schema defined in Appendix G-B to ICAO EUR Doc 020 (EUR AMHS Manual).

4.1.11 In order to access the information at local Co-operating and Adjacent DSAs for testing, validation and checking purposes, it is strongly recommended that implementations incorporate an Operational Personnel DUA as specified in ICAO Doc 9880 Part IV [3] as a minimum.

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

4.1.13 It is noted that communications between EDS peers occur in bursts during distribution of information.

Pan-European Network Service

4.1.14 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:

- ANSP Test Messaging VPN, for validation and test purposes
- ANSP Operational Messaging VPN, for operations

Virtual Private Network/Internet

4.1.15 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 on Internet Protocol Security (IPSec) and requires the negotiation of additional VPN-related parameters between the parties involved.

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

4.2 Peers

4.2.1 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; operation *dSABind* in case of DSP and operation *dSAShadowBind* in case of DISP.

4.2.2 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.

4.2.3 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 and the TCP port. Depending on the 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.

4.2.4 Table 1 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 TCP Port IPv4 Address		

Table 1: Peer Parameters

4.2.5 The parameters of the Central European DSA are provided by the Central Administrator. The operational facility is known by the value *O=EUXX*.

4.2.6 The Operator of a Co-operating or Adjacent DSA shall define the related parameters in accordance with the provisions given below, except for the password which is provided by the Central Administrator in order to ensure a minimum password complexity.

4.2.7 The distinguished name of the operational DSAs shall be represented by the attribute type *organization* taking the value of the location indicator of the respective COM Centre, e.g. *O=EDDD.*

4.2.8 The presentation, session and transport selectors are proposed to be absent. Values may be defined by mutual agreement.

4.2.9 The network address consists of the TCP port and the IPv4 address. The potential range of IP addresses is restricted by the common underlying network infrastructure in use. Within the network of the State or Organisation operating the Co-operating or Adjacent DSA the agreed TCP port and IP address may be mapped to a different IP address and different TCP port in line with local requirements.

Note.– The detailed way and particular steps required to configure the peer parameters depend on the implementation.

Shadowing

4.2.10 Shadowing using DISP is the preferred way 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 3.2.

4.2.11 Before shadowing takes place between two DSAs, an agreement covering the terms of the shadowing is required. The shadowing agreement established off-line between the supplier and the consumer defines:

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

4.2.12 Table 2 provides an overview of 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	
Update Mode	Supplier Initiated, On Change	
Access Point	Central European DSA (See Peers)	

Table 2: Shadowing Parameters

4.2.13 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 full update.

Note.– The detailed way and particular steps required to configure shadowing depend on the implementation.

Chaining

4.2.14 Chaining using DSP is a secondary means for distribution of information. The Co-operating or Adjacent DSA triggers this activity as given in section 3.3.

4.2.15 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.

4.2.16 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.

4.2.17 Table 3 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 3: Knowledge Reference Parameters

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

4.3 Users

4.3.1 Although the EDS user interface describes the relation between the Central European DSA and the Co-operating or Adjacent DSAs, this section addresses users of the EDS accessing the information stored within the EDS through a Directory User Agent connected to the local DSAs.

4.3.2 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 DNs 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. As a matter of principle, users always bind to their local Co-operating, Adjacent or a subordinate DSA.

4.3.3 Table 4 provides an overview on the parameters required to setup users. This table could be used to exchange user parameters.

Parameter	User
Distinguished Name	See below
Password	See below

Table 4: User Parameters

4.3.4 The Operational Concept of EDS identifies two types of users:

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

4.3.5 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. End users are managed by the respective Directory Management Domain (DMD) to which they are allocated.

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

4.3.6 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 to the background area of EDS. After successful registration, the Central Administrator creates a user entry for the respective Co-operating or Adjacent Operator, and provides him with his

DN and his initial password. Co-operating and Adjacent Operators may perform interrogation and modification operation on their own entry, allowing them to change their password.

4.3.7 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 systems.

4.3.8 It is noted, that in the intermediate and final step of EDS, Co-operating Operators can perform modification operations to their data in the background area of EDS, located at the Central European DSA only. The background area is not utilised in the initial step of EDS.

5 Trouble Shooting

5.1 General

5.1.1 This chapter provides considerations and basic advice for the purpose of trouble shooting.

5.1.2 Due to the complexity and distributed nature of the overall system there are several potential reasons in case 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.

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

5.2 Sources of Malfunction

5.2.1 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 entities tries to establish communication for the exchange of information. The bind operation or a subsequent shadowing or chaining operation could fail.

5.2.2 Basically two scenarios need to be considered in case of failures:

- Establishment of association (especially after setup):
  - The association between the Central European DSA and the Co-operating or - Adjacent DSA could not be established.
- Exchange of information:
  - An operation following the successful bind operation fails.

5.2.3 The establishment of an association through the bind operations *dSABind* (for DSP) or dSAShadowBind (for DISP) could fail for the following main reasons (bottom-up):

- A device is disconnected.
  After installation a device such as a server, router, firewall, etc. might not be properly connected to the network. Ensure that all devices involved in end-to-end communication are properly connected to the network(s).
- A device is not running properly.
  The start-up of a device might fail. Ensure that all devices involved in end-to-end communication are up and running.
- VPN setup is not aligned or inaccurate.
  In case a VPN is used, the VPN setup is an essential prerequisite for end-to-end communication. Ensure that the VPN is configured in accordance with the agreed parameters.
- Network security system blocks TCP port or IP address.
  A network security system such as a security appliance, firewall or proxy prevents end-to-end communication by blocking one of the TCP ports or IP addresses. Ensure that

any involved network security system is configured to support the TCP ports and IP addresses listed in Table 1.

- Mapping of TCP port or translation of IP address is not aligned or inaccurate.
  In case mapping of TCP port or translation of IP address appears, the configuration of involved devices have to be configured in accordance with the mapping of TCP ports and translation of IP addresses. Ensure that any mapping of TCP ports or translation of IP addresses is reflected in the communication setup of the involved components.
- The configuration of DSAs is not aligned or inaccurate.
  The peer DSAs have to implement the parameters listed in Table 1 considering any mapping of TCP ports or translation of IP addresses that appear in the local network infrastructure. Ensure that the DSAs are configured using the parameters listed in Table 1 and that any mapping of TCP ports or translation of IP addresses is considered in local DSA setup. Ensure that the remote DSA is reachable (e.g. network ping).
- The underlying network infrastructure is (temporarily) unavailable.
  It is not possible to establish end-to-end communication at the network level or a VPN could not be established. Ensure that end-to-end communication is possible and that the other end system is reachable (e.g. network ping).
- The Co-operating or Adjacent DSA is not available.
  The Co-operating or Adjacent DSA does not initiate or does not respond to bind requests. Ensure that the DSA is configured in accordance with the parameters listed in Table 1 taking into account mapping of TCP ports and translation of IP addresses with the local network infrastructure. Ensure that the credentials, i.e. distinguished names and passwords, are configured accordingly.
- The Central European DSA is not available.
  The Central European DSA does not initiate or does not respond to requests. Ensure that the local DSAs are configured in accordance with the parameters listed in Table 2 taking into account mapping of TCP ports and translation of IP addresses with the local network infrastructure. Ensure that the credentials (distinguished name and password) are configured accordingly.

5.2.4 Once an association has been established successfully a subsequent Directory operation such as *coordinateShadowUpdate*, *updateShadow*, *chainedRead*, *chainedList*, etc. could fail for the following main reasons:

- Network or device failed temporarily.
  Even though the bind operation was successful, any subsequent operation could fail as a result of a temporary outage of the network or a device involved in end-to-end communication. Ensure that all components are in operation, that end-to-end communication is possible and that the other end system is reachable (e.g. network ping).
- The Central European DSA, the Co-operating or Adjacent DSA refuses exchange of information.
  In order to perform replication or chained operations the DSAs have to be configured accordingly. Ensure that the configuration for replication and chaining of both DSAs is aligned and in accordance with the parameters listed in Table 2 (replication) or Table 3 (chaining).

5.3 Analysis

5.3.1 This section describes approaches for analysis in case of malfunction. The approaches make use of the Directory System Agent, Directory User Agent or tools that may be available

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

5.3.1 Directory System Agent

5.3.1.1 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.

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

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

5.3.2 Directory User Agent

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

5.3.2.2 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 DSA.

5.3.3 Network Analysis Tool

5.3.3.1 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.

5.3.3.2 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.

5.3.3.3 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.

6 Assessment of impact of modifications to the Directory Schema

6.1 General

6.1.1 All systems and users involved in the European Directory Service (EDS) have to be aware of the Directory schema in order to enable the exchange and the use of information made available by EDS. The directory schema specifies the objects contained in EDS by a set of data structures and rules. End users often have even to be aware of semantics in order to make use of the information.

6.1.2 Modifications to the Directory schema of EDS can have an impact to the implementations of DSAs and DUAs depending on the approach implemented for handling of the Directory schema. In case the Directory schema is fixed by the implementation (software), modifications to the Directory schema most probably imply adjustments of the implementation. In case the Directory schema is subject to configuration or even supplied by Directory means, modifications of the Directory schema usually have no impact to the implementation. With regard to EDS the Central European DSA, the Co-operating DSA and the Adjacent DSA as well as any generic DUA fall into this category.

6.1.3 Entities interpreting the Directory information semantically, such as users retrieving information by a DUA for further processing, depend on their knowledge on the Directory schema and on the semantics of the information. It is expected that modifications to the Directory schema have a significant impact to those kinds of implementations. However, such implementations are considered as a local matter.

6.1.4 In any case, modifications to the Directory schema need to be well-coordinated. Thus, any future modification of the Directory schema requires:

- a change process as defined in the EUR AMHS Manual and the approval by AST TF based on Change Proposals (CP);
- an assessment on the impact of the proposed modification; and
- a synchronisation of the implementation based on the results of the assessment.

6.1.5 The following sections focus on following aspects:

- Implementations of DSAs,
- Implementations of DUAs,
- Kind of modification.

6.2 Implementations of DSAs

6.2.1 The major difference to X.400/AMHS and advantage of X.500 DISP (Directory Information Shadowing Protocol) is the fact that the schema definition is part of the replication. Using DISP the Central European DSA replicates the schema in use prior to replicate the information. With this, Co-operating and Adjacent DSAs can receive the Directory schema by means of DISP.

6.2.2 In order to avoid complicated international procedures for Directory schema modifications (between the Central European DSA and the Co-operating and Adjacent DSAs), it is highly recommended that all DSA implementations support DISP and process the replicated Directory schema.

6.2.3 If there are serious reasons for a DSA implementation to ignore the replicated schema, then this DSA implementation should be tolerant, accepting and storing "unknown" elements on replication or as last resort ignore those elements as a minimum requirement.

6.2.4 Existing Co-operating and Adjacent DSAs in operation make use of the replicated schema definition and are, to the extent possible, prepared for modifications of the schema definition.

6.2.5 Nevertheless, the impact of a proposed modification shall be tested and assessed in the European EDS Test environment before implementing operationally.

6.3 Implementations of DUAs

6.3.1 Implementations of DUAs are by nature more sensitive to modifications of the schema definition than DSAs. It is supposed that most modifications to the schema definition require the adaption of the respective DUA implementation.

6.3.2 Adding new elements should not harm the operation of DUAs. But DUAs might use (system DUA) or display properly (human DUA) new elements only after adaption.

6.3.3 Modifications to the schema definition can impact the implementations of DUAs depending on the kind of modifications.

6.4 Kind of Modification

6.4.1 Taking into account DSA implementations ignoring the replicated schema definition, three basic kinds of modifications to the schema definition need to be looked at:

- potentially harmless,
- potentially harmful, and
- conflicting.

6.4.2 Harmless Modification

This kind of modification is expected to cause no or very limited issues in implementations of DSAs and DUAs, and thus might be introduced with limited synchronisation and short lead times.

6.4.3 Modifications of this kind are for example:

- Adding a new, structural or auxiliary object class
- Adding a new attribute type based on standard types
- Adding an attribute type to an existing object class
- Adding a new sub-tree or introduce new elements in an existing sub-tree (structure rule)

6.4.4 Harmful Modification

This kind of modification is expected to potentially cause issues in at least some implementations of DSAs and DUAs. It is proposed to avoid such modifications. If necessary, this kind of modification requires co-ordination and synchronisation. A staged approach (introduction of new elements in phase 1, removal of existing elements in phase 2) might be suitable to mitigate the impact.

6.4.5 Modifications of this kind are for example:

- Removal of a (mandatory) attribute type from an object class
- Removal of an object class
- Alteration of a structure rule

6.4.6 Conflicting modifications

This kind of modification is expected to potentially cause serious issues to implementations of DSAs and DUAs. This kind of modification must not occur and shall be replaced by modifications of the first two categories.

6.4.7 Modifications of this kind are for example:

- Modification of the definition of an existing attribute type
- Modification of the type of an existing object class (structural, auxiliary)
- Modification of the OID of an existing attribute type, object class or name form
- Making an optional attribute mandatory and vice versa
- Using non-standard syntaxes and matching rules

Standard syntaxes and matching rules as included in ISO/IEC 9594-6 (ITU-T X.520) are expected to be available in a wide range of commercial off-the-shelf products. Non-standard syntaxes however might not be available in implementations and require modifications to the implementations.

END of Appendix G-A