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~~Identifier Registration

[Approved by the Secretary General
and published under his authority]

Second ~~First~~ Edition (Proposed Draft) — ~~2010~~2015

International Civil Aviation Organization

Published in English only by the
INTERNATIONAL CIVIL AVIATION ORGANIZATION
999 University Street, Montréal, Quebec, Canada H3C 5H7

For ordering information and for a complete listing of sales agents
and booksellers, please go to the ICAO website at www.icao.int

Doc 9880, ***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~~Identifier Registration***
Order Number: 9880P4
ISBN 978-92-9231-531-3

AMENDMENTS

Amendments are announced in the supplements to the *Catalogue of ICAO Publications;* the Catalogue and its supplements are available on the ICAO website at www.icao.int. The space below is provided to keep a record of such amendments.

RECORD OF AMENDMENTS AND CORRIGENDA

AMENDMENTS		
No.	Date	Entered by

CORRIGENDA		
No.	Date	Entered by

~~TABLE OF CONTENTS~~

TABLE OF CONTENTS

Page

FOREWORD

The first Edition of this manual ~~amends~~ amended and ~~replaces~~ replaced the third edition of the *Manual of Technical Provisions for the Aeronautical Telecommunication Network (ATN)* (Doc 9705). This manual is a result of ongoing validation and operational experience gained during implementation of elements of the ATN. Amendments were reviewed at the first meeting of the Aeronautical Communications Panel (ACP) Working Group of the Whole in June 2005 and further updated at the ACP Working Group N/6 meeting held in July 2006. Relevant background material is available on the website www.icao.int/anb/panels/acp. The present Edition incorporates further Amendments developed by the ACP Working Group M (Maintenance) since publication of the first Edition.

This manual contains the detailed technical specifications for the ATN based on relevant standards and protocols established for open systems interconnection (OSI) by the International Organization for Standardization (ISO) and the Telecommunication Standardization Sector of the International Telecommunication Union (ITU-T). A separate manual, the *Manual on the Aeronautical Telecommunication Network (ATN) using Internet Protocol Suite (IPS) Standards and Protocols* (Doc 9896), addresses detailed technical specifications for the ATN based on standards developed for the IPS by the Internet Society (ISOC). Standards and Recommended Practices (SARPs) for the ATN/IPS are contained in Annex 10 — *Aeronautical Telecommunications,* Volume III — *Communication Systems.* Where necessary and to avoid duplication of material, Doc 9896 refers to this manual.

Editorial practices in this manual are as follows:

- The detailed technical specifications in this manual that include the operative verb "shall" are essential to be implemented to secure proper operation of the ATN.

- The detailed technical specifications in this manual that include the operative verb "should" are recommended for implementation in the ATN. However, particular implementations may not require this specification to be implemented.

- The detailed technical specifications in this manual that include the operative verb "may" are optional.

This manual is published in the following parts:

Part I: Air-Ground Applications (replaces Doc 9705, Sub-volume II)

Part II: Ground-Ground Applications — Air Traffic Services Message Handling Services (ATSMHS) (replaces Doc 9705, Sub-volume III)

Part III: Upper Layer Communications Service (ULCS) and Internet Communications Service (ICS) (replaces Doc 9705, Sub-volume IV and Sub-volume V)

Part IV: Directory Services, Security ~~Services~~ and ~~Systems Management~~Identifier Registration (replaces Doc 9705, Sub-volumes I, ~~VI,~~ VII, VIII and IX)

Structure of Part IV:

Chapter 1 INTRODUCTION contains the purpose and structure, and a summary of the functionality offered by each of the Chapters of this Part of Doc 9880 ~~the ATN directory service~~

Chapter 2 DIRECTORY SERVICES, provides the detailed technical specifications for the ATN directory services~~SYSTEM LEVEL PROVISIONS, provides a high level specification of the application and of the environment in which it operates~~

Chapter 3 SECURITY SERVICES, provides the detailed technical specifications for the ATN security services~~DIRECTORY OBJECT CLASS AND ATTRIBUTES SPECIFICATION contains the definition of the objects and attributes that may be used within the directory service~~

Chapter 4 IDENTIFIER REGISTRATION, provides the registration of ATN identifiers and associated provisions~~ATN DIRECTORY SYSTEM SCHEMA, specifies the contents and structure of the directory information base~~

~~Chapter 5 ATN DIRECTORY PROTOCOL, specifies the protocol profiles used by directory services~~

ACRONYMS

The acronyms used in this manual are defined as follows:

ACSE	Association control service element
AE	Application entity
AF	AFTN-form (address)
AFTN	Aeronautical fixed telecommunication network
AMHS	ATS message handling system
APDU	Application protocol data unit
ASN.1	Abstract syntax notation One
ATN	Aeronautical telecommunication network
ATN DIR	ATN directory service(s)
ATS	Air traffic services
ATSMHS	ATS message handling services
CCITT	Consultative Committee of International Telegraph and Telephone
DAP	Directory access protocol
DIB	Directory information base
DISP	Directory information shadowing protocol
DIT	Directory information tree
DMD	Directory management domain
DOP	Directory operational binding protocol
DSA	Directory system agent
DSP	Directory system protocol
DUA	Directory user agent
ICS	Internet communications service
IEC	International Electrotechnical Commission
IPS	Internet protocol suite
ISO	International Organization for Standardization
ISP	International standardized profile
ISPICS	ISP implementation conformance statement
IPv4	Internet protocol version 4
IPv6	Internet protocol version 6
ITU	International Telecommunication Union
ITU-T	International Telecommunication Union — Telecommunications Standards
MD	Management domain
MHS	Message handling system
MS	Message store(s)
ROSE	Remote operations service element
RTSE	Reliable transfer service element
TCP	Transmission control protocol

THIS PAGE LEFT BLANK INTENTIONALLY

Chapter 1

INTRODUCTION

1.1 OVERVIEW

1.1.1 General

Included in this part of Doc 9880 are technical provisions for:

a) Directory Services;

b) Security Services;

c) Identifier Registration

1.1.2 Directory Services

The ATN directory service (ATN DIR) allows ATN users to obtain directory information about ATN users, applications and services participating in the ATN. It is an application provided by the implementation over the ATN internet communication services or over the ATN internet protocol suite (IPS) of the directory services specified in ISO/IEC 9594/ITU-T X.500 Series, and complemented by the additional requirements specified in Chapter 2.

1.1.3 Security Services

The ATN security services are intended to support operational requirements for the secure exchange of ATS information via the ATN and for protection of ATN resources from unauthorized access. The ATN security services will accommodate mobile as well as fixed users of the network.

> *Note: Detailed technical specifications for ATN security services are under development by update of the technical provisions included in Doc 9705 Sub-Volume VIII, referred to in the Foreword above. When completed, these specifications will be provided in Chapter 3.*

1.1.4 Identifier registration

The ATN identifier registration acts as a central repository for common identifiers used in the ATN. This includes object identifiers (OIDs), application identifiers and other common identifier information. The purpose of this repository is to ensure uniqueness and consistency of the allocated identifiers. The ATN identifier registration is included in Chapter 4.

1.2 REFERENCES

1.2.1 Throughout this manual, any references to the ATN DIR technical provisions are references to Chapter 2 of this part of Doc 9880.

THIS PAGE LEFT BLANK INTENTIONALLY

Chapter 2

DIRECTORY SERVICES

2~~1~~.1 ~~OVERVIEW~~INTRODUCTION

2.1.1 Overview

2.1.1.1 The ATN directory service (ATN DIR) application allows ATN users to obtain directory information about ATN users, applications and services participating in the ATN. The ATN DIR is composed of three parts: a directory information base, directory system agents (DSAs) and directory user agents (DUAs).

2.1.1.2 The ATN DIR provides generic directory services over the ATN internet. It may also be used as a directory system supporting user applications communicating over the ATN. This may be achieved, for example, by means of application programmme interfaces.

2.1.1.3 The ATN DIR is provided by the implementation over the ATN internet communication services of the directory services specified in ISO/IEC 9594 and CCITT or ITU-T X.500, and complemented by the additional requirements specified in this manual. The ISO/IEC directory services international standards and the ITU-T X.500 series of recommendations (1993 or later) are in principle aligned with each other. However, there are a small number of differences. In this manual, reference is made to the relevant ISO International Standards and ISPs where applicable.

2.1.2 Terminology

2.1.2.1 The classifications defined in the referenced ISPs and PICS in the base standards are used to express conformance requirements — i.e. static capability — in this manual. These classifications include the following elements, of which the complete definition may be found in each referenced document:

a) **mandatory (full) support (M).** The support of the feature is mandatory for all implementations;

b) **optional support (O).** The support of the feature is left to the implementer;

c) **conditional support (C).** The requirement to support the item depends on a specified condition. The condition and the resulting support requirements are stated separately;

d) **excluded (X).** This feature is not allowed in implementation;

e) **out of scope (I).** Support of this feature is outside of the scope of this part of the specification; and

f) **not applicable (-).** The item is not defined in the context where it is mentioned. There is no support requirement. The occurrence of “not applicable” is mainly due to the format of the tables in the profile or PICS requirements list.

2.1.3 ATN DIR model

2.1.3.1 A directory is a collection of systems that cooperate to hold a logical database of information about a set of objects in the real world. The users of a directory, including people and computer programs, can read or modify the information, or parts of it, subject to having permission to do so. Each user accesses the information using a DUA which is considered to be an application process. These concepts are illustrated in Figure 2~~1~~-1.

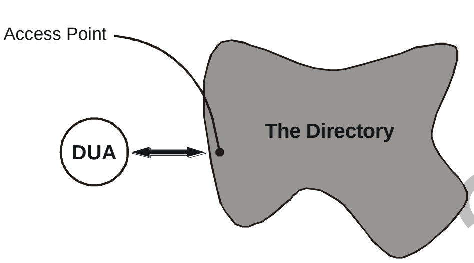

Figure 2-1~~1-1~~. Access to the ATN DIR

2.1.3.2 The information held in the ATN directory is collectively known as the directory information base (DIB). The DIB contains an entry for each real-world object (person, application, locality, etc.) represented in the directory. Entries are organized in such a way as to be directly identified using the directory name of the real-world object that represents them.

2.1.3.3 The structure of the DIB, called the directory information tree (DIT), defines a hierarchy of entries contained in the directory. The position of an entry in the DIT hierarchy determines that entry's directory name. The information content of each entry is defined by one or more object classes to which the entry belongs. An object class defines the information content of an entry as a set of attributes. Each attribute is a piece of information about the real world object or its entry. Attributes are defined by an attribute type (defining the semantics of the attribute) and an attribute syntax that enables extraction and testing of the value of the attribute. A number of matching rules are defined for each attribute syntax to enable testing of attributes values during the execution of directory operations. This allows users to select one or more directory entries based on the entry's content. A directory schema defines the object classes, attribute types, attribute syntaxes and matching rules of a part of the DIB.

2.1.3.4 The functional model of the ATN DIR is shown in Figure 2~~1~~-2.

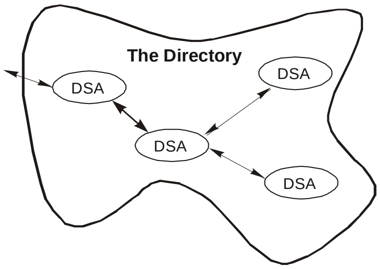

Figure 2-2~~1-2~~. Functional model of the ATN DIR

2.1.3.5 A DSA is an ATN application process which is a part of the directory and whose role is to hold, and to provide access, to the DIB for DUAs and/or other DSAs. A DSA may store fragments of the DIB in its local database. It may also interact with other DSAs to carry out requests concerning other fragments of the DIB. This is called “chaining”. Alternatively, the DSA may direct a user (or another enquiring DSA) to a further DSA which can help carry out the request. This is called “referral”.

2.1.3.6 A set of one or more DSAs and zero or more DUAs managed by a single organization may form a Directory Management Domain (DMD). The DSAs and DUAs of different DMDs interconnect in various ways to resolve user requests. DSAs of different DMDs may connect with each other to resolve chained directory operation on behalf of a user. Alternatively, a DMD may respond to one of its user’s requests by referring the user to connect directly with the DSA of another DMD. The particular choice is made on the basis of operational requirements.

2.1.3.7 The DUA interacts with the ATN DIR by communicating with one or more DSAs. A DUA need not be bound to any particular DSA and it may interact directly with various DSAs to make requests. For administrative reasons, it may not always be possible to interact directly with the DSA that is to carry out the request, e.g. to return directory information. It is also possible that the DUA may be able to access the entire DIB through a single DSA. For this purpose, DSAs may need to interact with each other by using chained operations.

2.1.3.8 A DSA is concerned with carrying out the requests of DUAs and with obtaining the information from other DSAs when it does not have the necessary information. It may take the responsibility to obtain the information by interacting with other DSAs on behalf of the DUA.

2.1.3.9 The ATN directory is supported by several different protocols: the directory access protocol (DAP); the directory system protocol (DSP); the directory information shadowing protocol (DISP); and the directory operational binding protocol (DOP). This manual provides specifications of DAP and DSP for use in the ATN. DISP is not profiled, but indications as to when it should be used are given. DOP is not profiled.

2.1.3.10 The DAP and DSP profiles are based on the requirements of ISO/IEC 13248-1 (*Directory Access Protocol — Protocol Implementation Conformance Statement*) which is equivalent to ITU-T Rec. X.583 and ISO/IEC 13248-2 (*Directory System Protocol — Protocol Implementation Conformance Statement*) which is equivalent to ITU-T Rec. X.584, and ISO/IEC 9594:1995. The high-level ATN directory protocol requirements expressed in this manual are:

a) conformance to the base standards by reference to ITU-T Recommendation X.583 | ISO/IEC 13248-1 and ITU-T Recommendation X.584 | ISO/IEC 13248-2 – PICS;

Note.— These are withdrawn standards but are available from the ITU-T website.

b) conformance to certain protocol extensions defined in ISO/IEC 9594:1995;

c) mandatory conformance to referral and distributed operations; and

d) conditional conformance to strong authentication and signed directory operations dependent on configuration and the availability of other security provisions.

2.1.3.11 Security

2.1.3.11.1 An overall strong security requirement is specified because some of the ATN directory data is highly critical to the operation (such as AMHS<>AFTN address translation data of ATSMHS) which must be protected against corruption or modification by unauthorised entities (e.g. by a masquerade attack). For this reason, strong authentication and signed operations, as specified by the [StrongSec] functional group or some other equivalent measures, need to be implemented depending on the configuration of DUAs and DSAs, and the relative security of the operational domain.

2.1.3.11.2 This specification therefore identifies an optional strong security functional group. Its use is dependent on a number of factors related to the directory's configuration and distribution and the operational domain in which the directory system operate. Requirements for this functional group are identified throughout this manual by means of the [StrongSec] predicate. In certain circumstances (e.g. where distributed operations are used) the DIB contents may be protected by the signed directory operations and responses contained in the [StrongSec] functional group. These effectively authenticate each operation and response individually. An alternative equivalent protection may be implemented by local or bilaterally agreed measures.

2.1.3.11.3 Authentication based on simple password protection is required as a minimum. Further (strong) authentication, if required, is a part of the [StrongSec] functional group which identifies suitable strong authentication protocol elements using standards-based techniques.

2.1.3.12 ATN DUA types

Formatted: Font: Italic

Formatted: Left

This section identifies three different profiles for ATN DUAs, each with access to a different required set of Directory operations.

> ***Administrative DUA.*** 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 to be subject to access controls for the modifying operations. It is also required to protect the DIB's data integrity and accuracy.
>
> ***Operational personnel DUA.*** An operational personnel DUA provides a (human) operational user with the limited range of directory operations enabling query of the directory without being granted access to the DIB modifying operations. Typical users of operational personnel DUAs include AMHS operators, AMHS users and users of end systems supporting ATN applications. Planners and management personnel also belong to this profile. This DUA requires guarantees of data integrity and accuracy.
>
> ***Autonomous operational DUAs.*** 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 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.

2.2 SYSTEM LEVEL PROVISIONS

Formatted: Level 1

2.2.1 ATN DIR system level requirements

2.2.1.1 The ATN DIR shall be implemented in conformance with provisions of this manual.

2.2.1.2 The systems comprising the ATN DIR shall themselves be comprised of two functional objects: DSAs and DUAs, the roles of which are described in ISO/IEC 9594-1:1995.

2.2.1.3 ATN DIR users shall access the ATN DIR using an ATN Directory User Agent (ATN DUA).

2.2.1.4 An ATN directory system agent shall support either the DAP the DSP or both, and optionally the DISP as specified in Section ~~Chapter~~ 2.5.

2.2.1.5 When used in support of the AMHS, an ATN DUA shall support the DAP, as specified in Section ~~Chapter~~ 2.5.

2.2.1.6 The ATN DIR shall be based on ISO/IEC 9594:1995 (ITU-T X.500:1993) specifications.

2.2.1.7 The ATN DIB shall be organized according to the structure of the ATN DIT as specified in Section ~~Chapter~~ 2.4.

2.2.1.8 The contents of the ATN DIB shall be capable of holding entries of the object classes defined in Section ~~Chapter~~ 2.4.

2.2.1.9 The ATN DSA shall support the PrintableString attribute syntax in order to ensure a minimum level of interworking.

2.2.1.9.1 The support for PrintableString attribute syntax is a mandatory requirement of ISO/IEC ISP 15126-1.

2.2.1.10 DUAs and DSAs shall protect the integrity of the DIB contents and the results of operations This may be achieved either by implementing the [StrongSec] functional group specified in this manual or may be achieved alternatively by local and bilateral arrangements appropriate to the operational domain(s).

2.2.2 Directory service deployment

2.2.2.1 A directory service implementation shall consist of one or more DSAs.

2.2.2.2 A user of the directory service shall make use of one or more DUAs.

2.2.2.3 If a DSA supports user access, it shall implement the DAP.

2.2.2.4 If a DSA supports access to other DSAs, it shall implement the DSP.

2.2.2.5 If a DSA provides or uses copies of DIB information with other DSAs, it shall implement the DISP.

2.2.2.6 It shall be valid to implement an ATN DUA or ATN DSA claiming conformance to this manual with or without the support of the strong security [StrongSec] functional group defined in this manual.

2.2.2.7 A DUA shall implement simple authentication for DAP.

2.2.2.8 A DSA shall implement simple authentication for DAP, DSP and DISP.

2.2.2.9 DUAs and DSAs implementing strong security [StrongSec] shall also implement strong authentication in the bind operation. This document profiles the protocol elements for [StrongSec] including the requirements for strong authentication. The cryptographic techniques to support the signed operations and responses of strong security are being developed. The cryptographic processing supporting strong authentication needs to be established by local or bilateral agreements.

2.2.2.10 If the [StrongSec] functional group is not implemented, then alternative, equivalent measures (e.g. data link and/or physical security) shall be implemented to protect the DIB content's integrity and accuracy, and the integrity and accuracy of the data returned in responses to DUAs.

2.2.2.11 A DUA shall either support the [StrongSec] functional group for DAP, or implement some other equivalent alternative security measures in case of local access.

2.2.2.12 A DSA shall either implement the [StrongSec] functional group for DAP, DSP and DISP for any configuration where remote access from DUAs or other DSAs is included, or implement some other equivalent alternative security measures in case of local access.

2.2.2.13 Operational personnel DUAs and autonomous operational DUAs shall be restricted to accessing the DIB using only the directory read operations — Read, Search and Compare.

2.2.2.14 An ATN DUA or ATN DSA implementation claiming conformance with the support of strong security shall implement all the associated requirements of this manual conditional directly or indirectly on the [StrongSec] predicate.

~~Chapter 3~~

2.3 DIRECTORY OBJECT CLASS AND ATTRIBUTES SPECIFICATION

Formatted: Level 1

2.3.1 Specification principles

2.3.1.1 Directory object classes are used to define the types of object that may be represented in the directory and their entry's information content. Separate object class requirements are specified for the DSA and the DUA. The DSA requirements specify the elements that all DSAs must be capable of storing and processing. The DUA requirements specify the minimum requirements placed on DUAs for accessing the DSAs.

2.3.1.2 The tables in this section express a "delta" requirement over and above the requirements of the referenced ISPs. It is assumed that implementation will conform to all the requirements of the referenced ISPs and base standards.

2.3.2 DSA object class requirements

2.3.2.1 The object classes used for ATN DSAs are derived from three sources:

a) object classes defined in the base ISO/IEC 9594-7:1995 and profiled in ISO/IEC ISP 15126-1;

b) object classes defined for use with the MHS extracted from withdrawn standard ISO/IEC ISP 11189; and

c) object classes specific to the ATN and defined in this manual.

2.3.2.2 DSA standard object classes

Formatted: Font: Italic

Formatted: Left

2.3.2.2.1 ATN DSAs shall support the object classes defined in ISO/IEC 9594-7:1995 as specified in ISO/IEC ISP 15126-1.

2.3.2.3 DSA object classes defined for the MHS

2.3.2.3.1 ISO/IEC ISP 11189 is an extension to profile ISO/IEC ISP 10616 (FDI11). ISO/IEC ISP 10616 is the object class profile for ISO/IEC 9594-7:1988 and has been superseded by ISO/IEC ISP 15126-1 due to the publication of ISO/IEC 9594-7:1995.

2.3.2.3.2 ATN DSAs shall support the MHS object classes indicated in Table 2~~3~~-1 with the syntax as defined in ISO/IEC 10021-2. (These object classes are defined in withdrawn standard ISO/IEC ISP 11189 (FDI2), Section A.6.4.1.2.)

2.3.2.3.2.1 ISO/IEC ISP 11189 defines specific object classes for use by the MHS. These object classes are based upon the standard object classes defined in Section 2.3.2.2 and extend those object classes.
2.3.2.3.2.2 ISO/IEC ISP 11189, Section A.6.4.1.2 defines the requirements for implementation of the object classes. ISO/IEC 10021-2 defines the required syntax for each object class.

2.3.2.3.2.3 Table 2-1~~3-1~~ is structured as a PRL derived from the ISPICS pro forma included in ISO/IEC ISP 11189 (FDI2). The columns “base”, “basic profile”, “profile DL FG” and “ISP” are extracted from ISO/IEC ISP 11189. The column “ATN DSA” specifies the static capability of an ATN DSA to contain, convey and handle attributes of the referenced object classes.

Table 2-1~~3-1~~. DSA support of object classes for the MHS

Ref. no.	*Object class*	*Base*	*Basic profile*	*DL profile FG*	*ATN DSA*
1	mhs-distribution~~L~~-list	O	O	M	M
2	mhs-message-store	O	O	-	M
3	mhs-message-transfer-agent	O	O	-	M
4	mhs-user	O	M	-	M
5	mhs-user-agent	O	O	-	M

2.3.2.4 DSA object classes defined for the ATN

2.3.2.4.1 ATN DSAs shall support the ATN-specific object classes as specified in Table 2~~3~~-2.

Table 2-2~~3-2~~. DSA support of object classes defined for the ATN

Ref.	*Object classes*	*ATN DSA*
1	atn-amhs-user	M
2	atn-organizational-unit	M
3	atn-organizational-person	M
4	atn-organizational-role	M
5	atn-application- entity	M
6	atn-certification-authority	M

Formatted: Font: Italic

Formatted: Left

Formatted: Font: Italic

Formatted: Left

7	atn-amhs-distribution~~L~~-list	M
8	atn-amhs-user-agent	M
9	atn-amhs-gateway	M
10	atn-aircraft	M
11	atn-facility	M
12	atn-amhsMD	M
13	atn-idrp-router	M
14	atn-dSA	M
15	atn-organization	M

2.3.2.4.2 The ATN DIB is composed of a set of specific object classes that are extensions of the basic object classes presented in Sections 2.3.2.2 to 2.3.2.3. This section defines new object classes and extends the standard object classes by adding attributes and mandating optional attributes.

2.3.2.4.3 The definition of the attributes comprising each object class is found in Section 2.4.4.

2.3.2.4.4 The ASN.1 of the ATN-specific object classes is found in Section 2.4.3.

2.3.3 DSA supported attribute types

2.3.3.1 DSA supported attribute types defined in ISO/IEC 9594-6:1995

Formatted: Font: Italic

Formatted: Left

2.3.3.1.1 ATN DSAs shall support the attribute types defined by ISO/IEC 9594-6:1995 as specified in ISO/IEC ISP 15126-1, Section A.6.4.1.2 as modified by Table 2~~3~~-3.

2.3.3.1.2 Table 2~~3~~-3 is structured as a PRL derived from the ISPICS pro forma included in ISO/IEC ISP 15126-1 (FDY 11). The columns “base” and “ISP” are extracted from ISO/IEC ISP 15126-1, and the column “ATN DSA” specifies the static capability of an ATN DSA to contain, convey and handle the referenced attributes within object classes to which they apply.

Table 2-3~~3-3~~. DSA support of ISO/IEC 9594-6 standard attribute types as specified in ISO/IEC ISP 15126-1

Ref no.	*Attribute type*	*Base*	*ISP*	*ATN DSA*	*Notes*
1	uniqueIdentifier	O	C1	M	Not present in 1988 edition.
2	userCertificate	O	C1	M	
3	cACertificate	O	C1	M	
4	authorityRevocationList	O	C1	M	
5	certificateRevocationList	O	C1	M	
6	crossCertificatePair	O	C1	M	

Ref no.	*Attribute type*	*Base*	*ISP*	*ATN DSA*	*Notes*
C1 = If p_strong_rep then M else O.					

2.3.3.2 DSA collective attribute types defined in ISP 15126-1

Formatted: Font: Italic

Formatted: Left

2.3.3.2.1 The ATN directory shall conform to ISO/IEC ISP 15126-1, Section A.6.4.2.3.

2.3.3.3 DSA attribute types for the MHS

Formatted: Font: Italic

Formatted: Left

2.3.3.3.1 ATN DSAs shall support the attribute types defined in ISO/IEC ISP 11189 (FDI2), Section A.6.4.2.2 as indicated in Table 2~~3~~-4.

2.3.3.3.2 Table 2~~3~~-4 is structured as a PRL derived from the ISPICS pro forma included in ISO/IEC ISP 11189 (FDI2). The columns “base” and “ISP” are extracted from ISO/IEC ISP 11189, and the column “ATN DSA” specifies the static capability of an ATN DSA to contain, convey and handle the referenced attributes.

Table 2-4~~3-4~~. DSA support of attribute types for the MHS

Ref. no.	*Attribute type*	*Base*	*ISP basic*	*ISP DL FG*	*ATN DSA*
1	mhs-acceptable-eits	O	O	-	O
2	mhs-deliverable-content-types	O	M	-	M
3	mhs-deliverable-classes	O	M	-	M
4	mhs-dl-archive-service	O	O	M	M
5	mhs-dl-members	O	I	M	M
6	mhs-dl-policy	O	I	M	M
7	mhs-dl-related-lists	O	I	M	M
8	mhs-dl-submit-permissions	M	I	M	M
9	mhs-dl-subscription-service	O	I	M	M
10	mhs-exclusively-acceptable-eits	O	M	-	M
11	mhs-maximum-content-length	O	M	-	M
12	mhs-message-store-dn	O	O	-	M
13	mhs-or-address	M	M	-	M
14	mhs-or-address-with-capabilities	O	O	-	M
15	mhs-supported-attributes	O	O	-	O
16	mhs-supported-automatic-actions	O	O	-	O
17	mhs-supported-content-types	O	O	-	M
18	mhs-supported-matching-rules			O	O

Ref. no.	*Attribute type*	*Base*	*ISP basic*	*ISP DL FG*	*ATN DSA*
19	mhs-unacceptable-eits	O	O	-	O

2.3.3.4 DSA attribute types defined for the ATN

2.3.3.4.1 An ATN DSA shall support the ATN-specific attributes defined in Section 2.4.4 as specified in Table 2~~3~~-5.

Formatted: Font: Italic

Formatted: Left

Table 2-5~~3-5~~. DSA support of attribute types defined for the ATN

Ref. no.	*Attribute type*	*ATN DSA*	*Notes*
1	atn-AF-address	M	See 4.4
2	atn-per-certificate	M	"
3	atn-der-certificate	M	"
4	atn-amhs-direct-access	M	"
5	atn-facility-name	M	"
6	atn-aircraftIDName	M	"
7	atn-version	M	"
8	atn-ipm-heading-extensions	M	"
9	atn-global-domain-identifier	M	"
10	atn-icao-designator	M	"
11	atn-net	M	"
12	atn-amhs-addressing-scheme	M	"
13	atn-amhsMD-naming-context	M	"
14	atn-maximum-number-of-body-parts	M	
15	atn-maximum-text-size	M	
16	atn-maximum-file-size	M	
17	atn-use-of-amhs-security	M	
18	atn-use-of-directory	M	
19	atn-group-of-addresses	M	

2.3.4 DUA object class requirements

2.3.4.1 The object classes supported by ATN DUAs are derived from three sources:

a) object classes defined in the base ISO 9594-7:1995 and profiled in ISO/IEC ISP 15126-1;

b) object classes defined for use with the MHS as extracted from withdrawn standard ISO/IEC ISP 11189; and

c) object classes specific to the ATN and defined in this manual.

2.3.4.2 The object classes defined for ATN DSAs in Section 2.3.2 delineate the type of information stored within the ATN DIR. The object classes defined for ATN DUAs specify the requirements for user access to that information. Necessarily, the specification of the DUA object class requirements is less comprehensive than the DSA requirements since DUAs need only be able to retrieve information relevant to its intended use.

2.3.4.3 The requirements stated in this section apply to the class of administrative DUAs that need to create, remove, read, modify and administer the entire contents of an ATN directory. Subsets of these object classes may apply to the other types of DUA that have a more limited and specific functionality (e.g. autonomous operational DUAs). These subsets are not defined in this manual.

2.3.4.4 Administrative DUA object classes defined in ISO/IEC 9594-7:1995

Formatted: Font: Italic

Formatted: Left

2.3.4.4.1 The DUAs shall conform to the object class requirements as defined in ISO/IEC ISP 15126-1, Annex B and as modified by Table 2~~3~~-6.

2.3.4.4.2 Table 2~~3~~-6 is structured as a PRL derived from the profile specification included in the ISPICS pro forma included in ISO/IEC ISP 15126-1 (FDY 11). The columns “base” and “ISP” are extracted from ISO/IEC ISP 15126-1, and the column “ATN DUA” specifies the static capability of an ATN DUA to convey and handle the referenced object classes.

Table 2-6~~3-6~~. DUA Support of ISO/IEC 9594-7:1995 standard object classes as specified in ISO/IEC 15126-1

Ref. No.	*Object class*	*Base*	*ISP*	*ATN DUA*
1	strongAuthenticationUser	O	C1	M
2	certificationAuthority	O	C1	M
C1: If p_strong_rep then M else O.				

2.3.4.5 DUA object classes defined for the MHS

Formatted: Font: Italic

Formatted: Left

2.3.4.5.1 ISO/IEC ISP 11189 is an extension to profile ISO/IEC ISP 10616 (FDI11). The ISO/IEC ISP 10616 object class profile has been superseded by ISO/IEC ISP 15126-1 due to the publication of a later version of ISO 9594-7.

2.3.4.5.2 ATN DUAs that support the AMHS shall support the object classes defined for the MHS as indicated in Table 2~~3~~-7 and with the syntax defined in ISO/IEC 10021-2. (These object classes are defined in withdrawn standard ISO/IEC ISP 11189 (FDI2), Section A.6.4.1.2.)

2.3.4.5.3 ISO/IEC ISP 11189, Section A.6.4.1.2 defines the requirements for implementation of the object classes. ISO/IEC 10021-2 defines the required syntax for each object class.

2.3.4.5.4 Table 2~~3~~-7 is structured as a PRL derived from the ISPICS pro forma included in ISO/IEC ISP 11189 (FDI2). The columns “base”, “basic profile”, “profile DL FG” and “ISP” are extracted from ISO/IEC ISP 11189. The column “ATN DUA” specifies the static capability of an ATN DUA to contain, convey and handle the referenced object classes.

Table 2-7~~3-7~~. DUA support of object classes for the MHS

Ref. no.	*Object class*	*Base*	*Basic profile*	*Profile DL*	*ATN DUA*
1	mhs-distribution-list	O	O	M	C2
2	mhs-message-store	O	O	-	C2

3	mhs-message-transfer-agent	O	O	-	C2
4	mhs-user	O	M	-	C2
5	mhs-user-agent	O	O	-	C2
C2: If the ATN DUA supports the AMHS then M else O.					

2.3.4.6 DUA supported ATN defined object classes

Formatted: Font: Italic

Formatted: Left

2.3.4.6.1 ATN DUAs shall support the ATN-specific object classes as specified in Table 2~~3~~-8.

Table 2-8~~3-8~~. DUA support of object classes defined for the ATN

Ref. no.	*Object classes*	*ATN DUA*	*Notes*
1	atn-amhs-user	M	Object class definition is in Section 2.4
2	atn-organizational-unit	M	“
3	atn-organizational-person	M	“
4	atn-organizational-role	M	“
5	atn-application-entity	M	“
6	atn-certification-authority	M	“
7	atn-amhs-distribution-list	M	“
8	atn-amhs-user-agent	M	“
9	atn-amhs-gateway	M	“
10	atn-aircraft	M	“
11	atn-facility	M	“
12	atn-amhsMD	M	“
13	atn-idrp-router	M	“
14	atn-dSA	M	“
15	atn-organization	M	“

2.3.5 DUA supported attribute types

2.3.5.1 DUA supported attribute types defined in ISO/IEC 9594-6:1995

Formatted: Font: Italic

Formatted: Left

2.3.5.1.1 ATN DUAs shall support the attribute type requirements as defined in ISO/IEC ISP 15126-1, Section B.6.4.2.1 as modified by Table 2~~3~~-9.

Table 2-9~~3-9~~. DUA support of standard attribute types

Ref no.	*Attribute type*	*Base*	*ISP*	*ATN DUA*

1	uniqueIdentifier	O	C1	M
2	uniqueMember	O	C1	M
3	userCertificate	O	C1	M
4	cACertificate	O	C1	M
5	authorityRevocationList	O	C1	M
6	certificateRevocationList	O	C1	M
7	crossCertificatePair	O	C1	M

C1: If p_strong_rep then M else O.

2.3.5.1.2 Table 2~~3~~-9 is structured as a PRL derived from the profile specification in the ISPICS pro forma included in ISO/IEC ISP 15126-1 (FDY 11). The columns “base” and “ISP” are extracted from ISO/IEC ISP 15126-1, and the column “ATN DUA” specifies the static capability of an ATN DUA to convey and handle the referenced attributes.

2.3.5.2 DUA support of collective attribute types defined in ISO/IEC ISP 15126-1

Formatted: Font: Italic

Formatted: Left

2.3.5.2.1 ATN DUAs shall conform to ISO/IEC ISP 15126-1, Section B.6.4.2.3.

2.3.5.3 DUA attribute types for the MHS

Formatted: Font: Italic

Formatted: Left

2.3.5.3.1 ATN DUAs shall support the attribute type requirements defined in Table 2~~3~~-10. (These attribute types are derived from those in withdrawn standard ISO/IEC ISP 11189 (FDI2), Section B.6.4.2.2.)

2.3.5.3.2 Table 2~~3~~-10 is structured as a PRL derived from the ISPICS pro forma included in ISO/IEC ISP 11189 (FDI2). The columns “base” and “ISP” are extracted from ISO/IEC ISP 11189, and the column “ATN DUA” specifies the static capability of an ATN DUA to contain, convey and handle the referenced attributes.

Table 2-10~~3-10~~. DUA attribute types for the MHS

Ref. no.	*Object class*	*Base*	*ISP basic*	*ISP DL FG*	*ATN DUA*
1	mhs-acceptable-eits	O	O	-	O
2	mhs-deliverable-content-types	O	M	-	C2
3	mhs-deliverable-classes	O	M	-	C2
4	mhs-dl-archive-service	O	O	M	C2
5	mhs-dl-members	O	I	M	C2
6	mhs-dl-policy	O	I	M	C2
7	mhs-dl-related-lists	O	I	M	C2
8	mhs-dl-submit-permissions	M	I	M	C2
9	mhs-dl-subscription-service	O	I	M	C2
10	mhs-exclusively-acceptable-its	O	M	-	C2
11	mhs-maximum-content-length	O	M	-	C2

Ref. no.	*Object class*	*Base*	*ISP basic*	*ISP DL FG*	*ATN DUA*
12	mhs-message-store-dn	O	O	-	C2
13	mhs-or-address	M	M	-	C2
14	mhs-or-address-with-capabilities	O	O	-	C2
15	mhs-supported-attributes	O	O	-	O
16	mhs-supported-automatic-actions	O	O	-	O
17	mhs-supported-content-types	O	O	-	C2
18	mhs-supported-matching-rules	O		O	O
19	mhs-unacceptable-eits	O	O	-	O
C2: If the ATN DUA is supporting the AMHS then M else O.					

2.3.5.4 *DUA supported ATN-specific attribute types*

Formatted: Font: Italic

Formatted: Left

2.3.5.4.1 ATN DUAs shall support the ATN-specific attributes listed in Table 2~~3~~-11.

Table 2-11~~3-11~~. DUA support of ATN-specific attribute types

Ref. no.	*Attribute type*	*ATN ~~DS~~DUA*	*Notes*
1	atn-AF-address	m	See 2.4.4.1
2	atn-per-certificate	m	See 2.4.4.2
3	atn-der-certificate	m	See 2.4.4.3
4	atn-amhs-direct-access	m	See 2.4.4.4
5	atn-facility-name	m	See 2.4.4.5
6	atn-aircraftIDName	m	See 2.4.4.6
7	atn-version	m	See 2.4.4.7
8	atn-ipm-heading-extensions	m	See 2.4.4.8
9	atn-global-domain-identifier	m	See 2.4.4.9
10	atn-icao-designator	m	See 2.4.4.10
12	atn-net	m	See 2.4.4.11
13	atn-amhs-addressing-scheme	m	See 2.4.4.12
14	atn-amhsMD-naming-context	m	See 2.4.4.13
14	atn-maximum-number-of-body-parts	m	See 2.4.4.14
15	atn-maximum-text-size	m	See 2.4.4.15
16	atn-maximum-file-size	m	See 2.4.4.16
17	atn-use-of-amhs-security	m	See 2.4.4.17
18	atn-use-of-directory	m	See 2.4.4.18

Ref. no.	*Attribute type*	*ATN ~~DSA~~DUA*	*Notes*
19	atn-group-of-addresses	m	See 2.4.4.19

~~Chapter 4~~

2.4 ATN DIRECTORY SYSTEM SCHEMA

Formatted: Level 1

2.4.1 Schema elements

2.4.1.1 The ATN directory schema includes the object class contents, directory schema operational object classes, directory schema operational attributes and the DIT. In general, a DSA must support all the schema elements required by DUAs that attach to it.

2.4.2 ATN directory object class contents

2.4.2.1 Section 2.3 specifies the required support of object classes and attributes for entries in the ATN DIR. This section specifies the ATN-specific attributes required for those object classes.

2.4.3 ASN.1 notation of ATN object class definitions

2.4.3.1 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 }
```

2.4.3.2 The ATN-specific object class atn-organizational-unit shall be defined by the ASN.1 syntax:

```
atn-organizational-unit  OBJECT-CLASS ::= {
        SUBCLASS OF         { organizationalUnit }
        MUST CONTAIN        {  }
        MAY CONTAIN         { atn-per-certificate |
                            atn-der-certificate |~~}~~
                            atn-facility-name }
        ID   id-oc-atn-OrganizationalUnit }
```

2.4.3.3 The ATN-specific object class atn-organizational-person shall be defined by the ASN.1 syntax:

```
atn-organizational-person OBJECT-CLASS ::= {
        SUBCLASS OF          { organizationalPerson }
        MUST CONTAIN        {  }
        MAY CONTAIN         { atn-per-certificate |
                            atn-der-certificate }
        ID   id-oc-atn-OrganizationalPerson }
```

2.4.3.4 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 }
```

2.4.3.5 The ATN-specific object class atn-application-entity shall be defined by the ASN.1 syntax:

```
atn-application-entity OBJECT-CLASS ::= {
        SUBCLASS OF     { applicationEntity }
        MUST CONTAIN {  }
        MAY CONTAIN     { atn-per-certificate |
                        atn-der-certificate |
                        atn-version }
        ID   id-oc-atn-ApplicationEntity }
```

2.4.3.6 The ATN-specific object class atn-certification-authority shall be defined by the ASN.1 syntax.

```
atn-certification-authority OBJECT-CLASS ::= {
        SUBCLASS OF     { certificationAuthority }
        KIND            AUXILIARY
        MUST CONTAIN {  }
        MAY CONTAIN     { atn-per-certificate |
                        atn-der-certificate }
        ID   id-oc-atn-certificationAuthority }
```

2.4.3.7 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~~L~~-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 }
```

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

```
atn-amhs-user-agent OBJECT-CLASS ::= {
        SUBCLASS OF    { mhs-user-agent }
        MUST CONTAIN { atn-ipm-heading-extensions }
        MAY CONTAIN    {  }
        ID   id-oc-atn-AmhsUserAgent }
```

2.4.3.9 The ATN-specific object class atn-amhs-gateway shall be defined by the ASN.1 syntax:

```
atn-amhs-gateway OBJECT-CLASS ::= {
        SUBCLASS OF    { applicationEntity }
        MUST CONTAIN { owner |
                        atn-ipm-heading-extensions }
        MAY CONTAIN    {mhs-maximum-content-length |
                        mhs-deliverable-content-types |
                        mhs-acceptable-eits |
                        mhs-exclusively-acceptable-eits |
                        mhs-or-addresses |
                        atn-AF-address }
        ID   id-oc-atn-AmhsGateway }
```

2.4.3.10 The ATN-specific object class atn-aircraft shall be defined by the ASN.1 syntax:

```
atn-aircraft OBJECT-CLASS ::= {
        SUBCLASS OF    { top }
        MUST CONTAIN { atn-aircraftIDName }
        MAY CONTAIN    { atn-per-certificate }
        ID   id-oc-atn-Aircraft }
```

2.4.3.11 The ATN-specific object class atn-facility shall be defined by the ASN.1 syntax:

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

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

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

2.4.3.13 The ATN-specific object class atn-idrp-router shall be defined by the ASN.1 syntax:

```
atn-idrp-router OBJECT-CLASS ::= {
        SUBCLASS OF        { device }
        MUST CONTAIN       { atn-net |
                             atn-per-certificate |
                             atn-version }
        MAY CONTAIN        { atn-der-certificate }
        ID   id-oc-atn-idrpRouter }
```

2.4.3.14 The ATN-specific object class atn-dSA shall be defined by the ASN.1 syntax:

```
atn-dSA OBJECT-CLASS ::= {
        SUBCLASS OF        { dSA }
        MUST CONTAIN       { atn-per-certificate |
                             atn-der-certificate |
                             atn-version }
        MAY CONTAIN        {  }
        ID   id-oc-atn-DirectorySystemAgent }
```

2.4.3.15 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-per-certificate }
        ID   id-oc-atn-Organization }
```

2.4.4 ASN.1 notation of ATN specific attribute types

2.4.4.1 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 }
```

2.4.4.2 The ATN-specific attribute atn-per-certificate shall be the octet string of the result from the PER encoding of a compressed ATN certificate, the syntax of which is to be developed.

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

2.4.4.2.1 The definition of the atn-per-certificate indicates the specific encoding of the atn-Certificate using packed encoding rules.

2.4.4.3 The ATN-specific attribute atn-der-certificate shall be the DER encoded certificate defined by the ASN.1 syntax, with the atn-der-certificate's value constructed for the "uncompressed certificate":

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

2.4.4.3.1 The certificate syntax is defined in ISO/IEC 9594, Part 8, Section 7.

2.4.4.3.2 The definition of atn-der-certificate indicates the specific encoding of the atn-Certificate using distinguished encoding rules.

2.4.4.4 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 }
```

2.4.4.5 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 }
```

2.4.4.6 The ATN-specific attribute atn-aircraftIDName shall be defined by the ASN.1 syntax:

```
atn-aircraftIDName           ATTRIBUTE ::= {
                             WITH SYNTAX INTEGER(0..2**24-1)
                             ID id-at-atn- aircraftIDName }
```

2.4.4.7 The ATN-specific attribute atn-version shall be defined by the ASN.1 syntax:

```
atn-version                  ATTRIBUTE ::= {
                             WITH SYNTAX INTEGER
                             ID id-at-atn-version }
```

2.4.4.8 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 }
```

2.4.4.9 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 }
```

2.4.4.10 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 }
```

2.4.4.11 The ATN-specific attribute atn-net shall be defined by the ASN.1 syntax:

```
atn-net                      ATTRIBUTE ::= {
                             WITH SYNTAX PrintableString(SIZE(1..19))
                             ID id-at-atn-Net }
```

2.4.4.12 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 }
```

2.4.4.13 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 }
```

2.4.4.14 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 }
```

2.4.4.15 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 }
```

2.4.4.16 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 }
```

2.4.4.17 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 }
```

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

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

2.4.4.19 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 }
```

2.4.5 Specific DIT structure for operational information

2.4.5.1 This section only deals with aspects of the DIT structure concerning directory internal administrative and operational information. The form of the DIT that is relevant for administrative entries and subentries and required by the administrative and naming authorities responsible for a given region/domain/subtree is specified with the help of:

a) name forms, which define which attributes are used to form the RDN of a subentry;

b) DIT structure rules, which define the hierarchical relationship of administrative entries and subentries.

2.4.5.2 Name forms

Formatted: Font: Italic

Formatted: Left

2.4.5.2.1 DSAs shall support the subentry NameForm as described in ISO/IEC ISP 15126-2, Section A.6.5.1.1.

2.4.5.2.2 Support of this name form by a DSA means that the following conditions are fulfilled:

a) the DSA supports the named object class as described in ISO/IEC ISP 15126-2, Section 7.1; and

b) the DSA is able to create a subentry of a specified object class, the RDN of which contains all mandatory attributes and zero or more of the optional attributes indicated in the name form.

Table 2-124~~-1~~. DSA support of name forms defined in ISO/IEC ISP 15126-2

Ref. no.	*Name form*	*Base*	*ISP*	*ATN directory*
1	subentryNameForm	O	M	M

2.4.6 Operational content of entries and subentries

2.4.6.1 ATN DSAs shall conform to the requirements of ISO/IEC ISP 15126-2, Sections 7.1, 7.2 and 7.5 regarding operational content object classes and operational attributes.

2.4.7 Content rules for the directory system schema

2.4.7.1 ATN DSAs shall conform to ISO/IEC ISP 15126-2, Section 7.3.

2.4.8 ATN DIT structure

2.4.8.1 The form of the DIT required by the ATN administrative and naming authorities responsible for a given State or region is specified with the help of:

a) name forms, which define which attributes are used to form the RDN of an entry; and

b) DIT structure rules, which define the hierarchical relationship of entries.

2.4.8.2 Name forms

2.4.8.2.1 ATN DSAs shall support the name forms specified in ISO/IEC ISP 15126-1, Section A.6.5.1.1 and with the modifications identified in Table 2-134~~-2~~.

2.4.8.2.1.1 Table 2-134~~-2~~ is structured as a PRL derived from the profile specification in the ISPICS pro forma included in ISO/IEC ISP 15126-1 (FDY 11). The column “base” and “ISP” are extracted from ISO/IEC ISP 15126-1, and the column “ATN DSA” specifies the static capability of a DSA to support these attributes in directory operations.

Table 2-134~~-2~~. ATN support of standard name forms

Ref. no.	*Name form*	*Base*	*ISP*	*ATN DSA*
1	countryNameForm	O	C8	M
C8: If p_firstlevel then M else O.				

Formatted: Font: Italic

Formatted: Left

2.4.8.2.2 ATN DSAs shall support the ATN-specific name forms defined for ATN-specific object classes as specified in Table 2-14~~4-3~~.

Table 2-14~~4-3~~. ATN-specific name forms

Ref. no.	*Name form*	*ATN DSA*
1	atnOrgUnitNameForm	M
2	atnOrgPersonNameForm	M
3	atnOrgRoleNameForm	M
4	atnApplEntityNameForm	M
5	atnAmhsDLNameForm	M
6	atnAmhsUANameForm	M
7	atnAmhsGatewayNameForm	M
8	atnAircraftNameForm	M
9	atnFacilityNameForm	M
10	atnAmhsMDNameForm	M
11	atnIdrpRouterNameForm	M
12	atnDSANameForm	M
13	atnOrgNameForm	M

2.4.8.2.3 ATN name forms shall comply with the following ASN.1 definitions:

```
atnOrgUnitNameForm          NAME-FORM  ::=  {
    NAMES                   atn-organizational-unit
    WITH ATTRIBUTES         { organizationalUnitName }
    ID                      id-nf-atnOrgUnitNameForm }

atnOrgPersonNameForm        NAME-FORM  ::=  {
    NAMES                   atn-organizational-person
    WITH ATTRIBUTES         { commonName }
    ID                      id-nf-atnOrgPersonNameForm }

atnOrgRoleNameForm          NAME-FORM  ::=  {
    NAMES                   atn-organizational-role
    WITH ATTRIBUTES         { commonName }
    ID                      id-nf-atnOrgRoleNameForm }

atnApplEntityNameForm       NAME-FORM  ::=  {
    NAMES                   atn-application-entity
    WITH ATTRIBUTES         { commonName }
    ID                      id-nf- atnApplEntityNameForm }

atnAmhsDLNameForm           NAME-FORM  ::=  {
    NAMES                      atn-amhs-distribution-list ~~distributionList~~
    WITH ATTRIBUTES            { commonName }
    ID                         id-nf-atnAmhsDLNameForm }
atnAmhsUANameForm                  NAME-FORM  ::=  {
    NAMES                      atn-amhs-user-agent
    WITH ATTRIBUTES            { commonName }
    ID                         id-nf-atnAmhsUANameForm }

atnAmhsGatewayNameForm             NAME-FORM  ::=  {
    NAMES                      atn-amhs-gateway
    WITH ATTRIBUTES            { commonName }
    ID                         id-nf-atnAmhsGatewayNameForm }

atnAmhsMDNameForm                  NAME-FORM  ::=  {
    NAMES                      atn-amhsMD
    WITH ATTRIBUTES            { commonName }
    ID                         id-nf-atnAmhsMDNameForm }

atnOrgNameForm                     NAME-FORM  ::=  {
    NAMES                      atn-organization
    WITH ATTRIBUTES            { ~~O~~organizationName }
    ID                         id-nf-atnOrgNameForm }

atnAircraftNameForm                NAME-FORM ::=  {
    NAMES                      atn-aircraft
    WITH ATTRIBUTES            {atn-aircraftIDName }
    ID                         id-nf-atnAircraftNameForm }

atnFacilityNameForm                NAME-FORM  ::=  {
    NAMES                      atn-facility
    WITH ATTRIBUTES            {atn-facility-name }
    ID                         id-nf-atnFacilityNameForm }

atnIdrpRouterNameForm              NAME-FORM  ::=  {
    NAMES                      atn-idrp-router
    WITH ATTRIBUTES            {commonName }
    ID                         id-nf-atnIdrpRouterNameForm }

atnDSANameForm                     NAME-FORM  ::=  {
    NAMES                      atn-dSA
    WITH ATTRIBUTES            {commonName }
    ID                         id-nf-atnDSANameForm }
```

2.4.8.3 ATN DSAs shall support the DIT structure specified in Table 2-15~~4-4~~.

Table 2-15~~4-4~~. ATN DIT structure

Structure element	*Structural object class*	*Superior structural element*	*Naming attribute*	*Notes*
0	root	-		
1	country	0,3	countryName	
2	organization	0, 1, 3	organizationName	
3	organizationalUnit	2	organizationalUnitName	
4	applicationProcess	2, 3, 8, 9, 10, 11	commonName	
5	applicationEntity	2, 3, 4, 8, 9, 10, 11	commonName	
6	atn-application-entity	2, 3, 4, 8, 9, 10, 11	commonName	2.4.3.5
7	atn-dSA	2, 3, 8, 9, 10, 11	commonName	2.4.3.14
8	atn-facility	2, 3, 10, 11	atn-facility-name	2.4.3.11
9	atn-aircraft	1, 2	atn-aircraftIDName	2.4.3.10
10	atn-organizational-unit	2, 11	organizationalUnitName	2.4.3.2
11	atn-organization	0, 1, 2	organizationName	2.4.3.15
12	atn-amhs-distribution-list~~distributionList~~	1, 2, 3, 8, 9, 10, 11, 15 ~~12, 13, 17~~	commonName	2.4.3.7
13	atn-amhs-user-agent	1, 2, 3, 8, 9, 10, 11, ~~12, 13, 18, 19~~15, 17, 21	commonName	2.4.3.8
14	atn-amhs-gateway	1, 2, 3, 8, 9, 10, 11, ~~13,~~15, 17, 21	commonName	2.4.3.9
15	atn-amhsMD	1, 2, 11~~13~~	commonName	2.4.3.12
16	atn-organizational-person	2, 3, 8, ~~9,~~ 10, 11	commonName	2.4.3.3
17	atn-organizational-role	2, 3, 8,~~9~~ 10, 11	commonName	2.4.3.4
18	atn-idrp-router	2, 3, 8, 9, 10, 11	commonName	2.4.3.13
19	device	2, 3, 8, 9, 10, 11	commonName	
20	organizational-person	2, 3, 8, 10,11	commonName	
21	organizational-role	2, 3, 8, 10,11	commonName	

2.4.8.4 ATN DSAs shall support the DIT structure found in Figure 2-3~~4-1~~ and Figure 2-4~~4-2~~.

2.4.8.5 In the event of a conflict between the actions implied by the figures and the table above, the table shall take precedence.

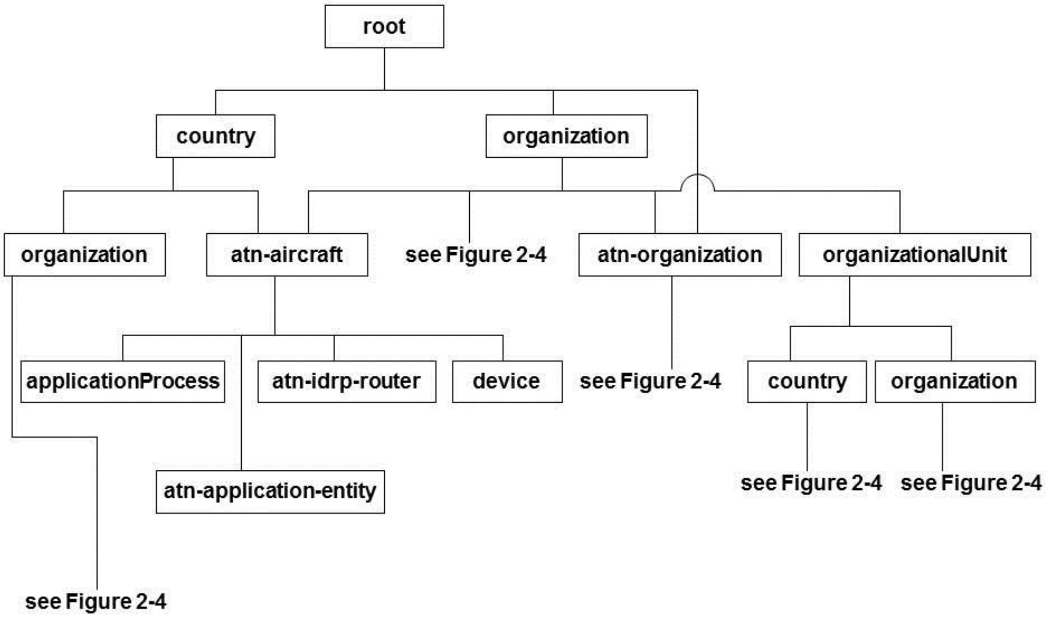

Figure 2-3~~4-1~~. Root level ATN DIT structure

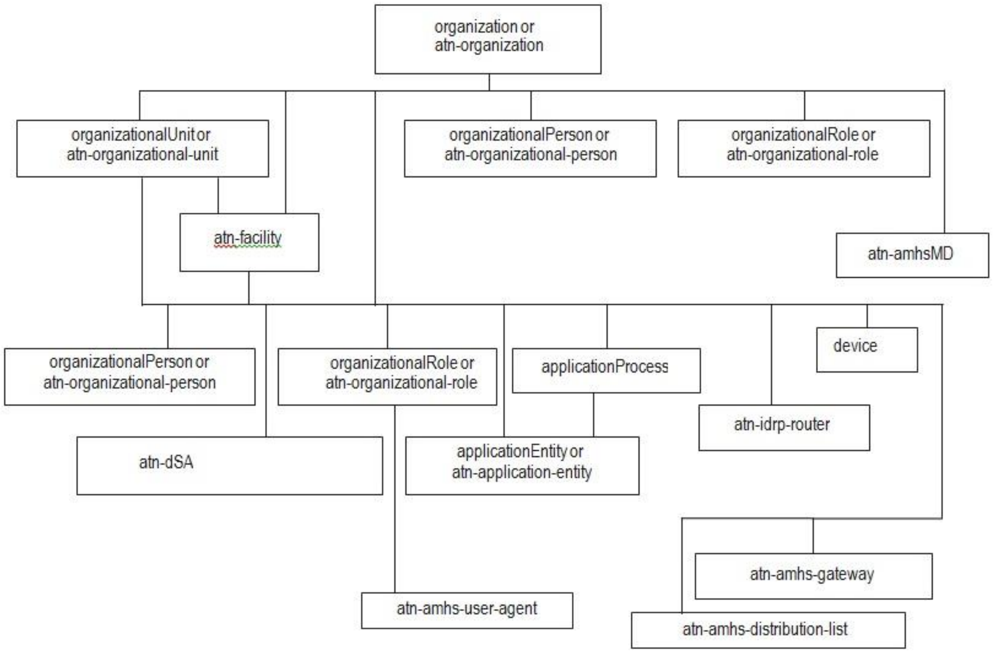

Figure 2-44~~-2~~. ATN organizational DIT structure

2.4.9 ATN directory matching rules

2.4.9.1 Matching directory strings for equality and substring

Formatted: Font: Italic

Formatted: Left

2.4.9.1.1 Two strings shall match for equality or substring, using a specified matching rule, if and only if:

a) they satisfy the syntax specified for the matching rule; and

b) they are identical when semantically compared name-by-name for each graphic character in the strings, subject to rules relating to:

1) handling of initial, middle, and final spaces; and

2) case if supported by the used character repertoire, as defined for the corresponding matching rule.

2.4.9.1.2 The matching of two strings that contain (unknown) characters in an unsupported character set shall be subject to local options.

2.4.9.1.3 The following character set specific rules shall apply.

2.4.9.1.3.1 These rules apply for TeletexStrings, BMPStrings and UniversalStrings.

2.4.9.1.3.2 Since “small ‘d’ with stroke” and “small ‘eth’, Icelandic” map to the same capital “capital ‘D’ with stroke, Icelandic ‘eth’” both corresponding lower case letters shall be taken as matching. This avoids TeletexString matching being intransitive.

2.4.9.1.3.3 The character “terminal sigma” shall match “small Greek letter sigma” and shall map to the same capital “capital Greek letter sigma”.

2.4.9.1.3.4 The omega and mu Greek letters in 103 shall match corresponding letters in 126.

2.4.9.1.3.5 The “soft hyphen” shall be ignored for matching purposes.

2.4.9.1.3.6 The “no-break space” shall be taken as equivalent to an ordinary space.

2.4.9.1.3.7 The “ohm sign” and “micro sign” shall match the corresponding Greek letters.

2.4.9.1.3.8 The “small sharp ‘s’, German” shall match with ‘ss’.

2.4.9.1.3.9 INCREMENT shall match with GREEK CAPITAL LETTER DELTA.

2.4.9.1.3.10 N-ary SUMMATION shall match with GREEK CAPITAL LETTER SIGMA.

2.4.9.2 Specific matching rules

Formatted: Font: Italic

Formatted: Left

2.4.9.2.1 ATN DSAs shall support the matching rules as specified in ISO/IEC ISP 15126-1, Section A.6.5.2 with the modifications indicated in Table 2-16~~4-5~~.

2.4.9.2.2 Table 2-16~~4-5~~ is structured as a PRL derived from the profile specification in the ISPICS pro forma included in ISO/IEC ISP 15126-1 (FDY 11). The columns “base” and “ISP” are extracted from ISO/IEC ISP 15126-1, and the column “ATN DSA” specifies the static capability of a DSA to support these attributes in directory operations.

Table 2-16~~4-5~~. ATN DSA matching rules specified in ISO/IEC ISP 15126-1

Ref. no.	*Matching rules*	*Base*	*ISP*	*ATN DSA*
1	caseIgnoreOrderingMatch	O	O	M
2	octetStringOrderingMatch	O	O	M
3	uniqueMemberMatch	O	C1	M
4	generalizedTimeOrderingMatch	O	O	M
C1: If p_strong_rep then M else O.				

2.4.9.2.3 ATN DSAs shall support the matching rules as indicated in Table 2-17~~4-6~~. (These matching rules are specified in withdrawn standard ISO/IEC ISP 11189, Section A.6.5.4.)

2.4.9.2.4 Table 2-17~~4-6~~ is structured as a PRL derived from the profile specification in the ISPICS pro forma included in ISO/IEC ISP 11189 (FDI2). The columns “base” and “ISP” are extracted from ISO/IEC ISP 15126-1, and the column “ATN DSA” specifies the static capability of a DSA to support these attributes in directory operations.

Table 2-17~~4-6~~. ATN DSA matching rules for the MHS

Ref. no.	*Matching rule*	*Base*	*ISP Basic*	*ISP AMR*	*ISP SMR*	*ISP DL*	*ATN DSA*
1	oRAddressCapabilitiesMatch	C9	C9	-	-	-	M
2	oRAddressElementsMatch	O	O	M	-	-	M
3	oRAddressMatch	C9	M	-	-	-	M
4	oRAddressSubstringElementsMatch	O	O		M		M
5	oRNameElementsMatch	O	O	M	-	-	M
6	oRNameExactMatch	C9	C9	-	-	M	M
7	oRNameMatch	O	O	M	-	-	M
8	oRNameSingleElementsMatch	O	O	M	-	-	M
9	orNameSubstringElementsMatch	O	O	-	M	-	M
C9: If there exists an attribute which uses it as an equality matching rule and that attribute is supported then M else O.							

2.4.10 Reference definition of ATN directory schema elements in ASN.1

```
ATNDirectoryObjectIdentifiers {iso(1) identified-organisation(3) icao(27) atn(0) objectIdentifiers(0) atnDirectory(0) }
DEFINITIONS AUTOMATIC TAGS ::=
BEGIN
--          Prologue
--          Exports everything

IMPORTS

--          Object Identifiers
            id-oc, id-at
            ….
            From ATNDirectoryObjectIdentifiers { iso(1) identified-organisation(3) icao(27) atn(0) objectIdentifiers(0)
atnDirectory(0) }

            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           ~~{ atn-per-certificate |~~
                                { 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-der-certificate |
                                atn-use-of-amhs-security |
                                atn-use-of-directory |
                                atn-group-of-addresses |
                                atn-AF-address }
          ID                    id-oc-atn-AmhsUser }

atn-organizational-unit OBJECT-CLASS ::= {
          SUBCLASS OF           { organizationalUnit }
          MUST CONTAIN          {}
          MAY CONTAIN           { atn-per-certificate |
                                atn-der-certificate |
                                atn-facility-name }
          ID                    id-oc-atn-OrganizationalUnit }

atn-organizational-person OBJECT-CLASS ::= {
          SUBCLASS OF           { organizationalPerson }
          MUST CONTAIN          {  }
          MAY CONTAIN           { atn-per-certificate |
                                atn-der-certificate }
          ID                    id-oc-atn-OrganizationalPerson }

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

atn-application-entity OBJECT-CLASS ::= {
          SUBCLASS OF           { applicationEntity }
          MUST CONTAIN          {  }
          MAY CONTAIN           { atn-per-certificate |
                                atn-der-certificate |
                                atn-version }
          ID                    id-oc-atn-ApplicationEntity }

atn-certification-authority OBJECT-CLASS ::= {
          SUBCLASS OF           { certificationAuthority }
          KIND                  AUXILIARY
          MUST CONTAIN          {  }
          MAY CONTAIN           { atn-per-certificate |
                        atn-der-certificate }
      ID                id-oc-atn-certificationAuthority }

atn-amhs-distribution-list OBJECT-CLASS ::= {
      SUBCLASS OF       { mhs-distribution-~~L~~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 }

atn-amhs-user-agent OBJECT-CLASS ::= {
      SUBCLASS OF       { mhs-user-agent }
      MUST CONTAIN      { atn-ipm-heading-extensions }
      MAY CONTAIN       {  }
      ID                id-oc-atn-AmhsUserAgent }

atn-amhs-gateway OBJECT-CLASS ::= {
      SUBCLASS OF       { applicationEntity }
      MUST CONTAIN      { owner |
                        atn-ipm-heading-extensions }
      MAY CONTAIN       { mhs-maximum-content-length |
                        mhs-deliverable-content-types |
                        mhs-acceptable-eits |
                        mhs-exclusively-acceptable-eits |
                        mhs-or-addresses |
                        atn-AF-address }
      ID                id-oc-atn-AmhsGateway }

~~atn-AmhsGateway OBJECT-CLASS ::= {~~
~~      SUBCLASS OF       { application-Entity }~~
~~      MUST CONTAIN      { owner |~~
~~                        mhs-deliverable-content-types |~~
~~                        protocolInformation |~~
~~                        mhs-deliverable-classes |~~
~~                        mhs-or-addresses |~~
~~                        atn-ipm-heading-extensions |~~
~~      MAY CONTAIN       { mhs-maximum-content-length |~~
~~                        mhs-deliverable-content-types |~~
~~                        mhs-acceptable-eits |~~
~~                        mhs-exclusively-acceptable-content-types |~~
~~                        mhs-or-addresses |~~
~~                        atn-AF-address }~~
~~      ID                id-oc-atn-AmhsGateway }~~

~~atn-aircraft OBJECT-CLASS ::= {~~
~~      SUBCLASS OF       { top }~~
~~          MUST CONTAIN { atn-aircraftIDName }~~
~~          MAY CONTAIN   { atn-per-certificate }~~
~~          ID                    id-oc-atn-Aircraft }~~

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

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

atn-idrp-router OBJECT-CLASS ::= {
          SUBCLASS OF    { device }
          MUST CONTAIN { atn-net |
                         atn-per-certificate |
                         atn-version }
          MAY CONTAIN    { atn-der-certificate }
          ID             id-oc-atn-idrpRouter }

atn-dSA OBJECT-CLASS ::= {
          SUBCLASS OF    { dSA }
          MUST CONTAIN { atn-per-certificate |
                         atn-der-certificate |
                         atn-version }
          MAY CONTAIN    { }
          ID             id-oc-atn-DirectorySystemAgent }

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

 -- ATN directory attribute types

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

          atn-per-certificate ATTRIBUTE ::= {
                    WITH SYNTAX                                       OCTET STRING
```

```
        ID id-at-atn-PerCertificate }

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

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

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

atn-aircraftIDName ATTRIBUTE ::= {
        WITH SYNTAX                                   INTEGER(0..2**24-1)
        ID id-at-atn-facilityName }

atn-version ATTRIBUTE ::= {
        WITH SYNTAX                                   INTEGER
        ID id-at-atn-version}

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

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

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

atn-net ATTRIBUTE ::= {
        WITH SYNTAX                                   PrintableString(SIZE(1..19))
        ID id-at-atn-Net }

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

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

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

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

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

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

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

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


-- Name forms
    atnOrgUnitNameForm                      NAME-FORM  ::=  {
            NAMES                           atn-organizational-unit
            WITH ATTRIBUTES                 { ~~O~~organizationalUnitName }
            ID                              id-nf-atnOrgUnitNameForm }

    atnOrgPersonNameForm                    NAME-FORM  ::=  {
            NAMES                           atn-organizational-person
            WITH ATTRIBUTES                 { commonName }
            ID                              id-nf-atnOrgPersonNameForm }

    atnOrgRoleNameForm                      NAME-FORM  ::=  {
        NAMES                               atn-organizational-role
        WITH ATTRIBUTES                     { commonName }
        ID                                  id-nf-atnOrgRoleNameForm }

    atnApplEntityNameForm                   NAME-FORM  ::=  {
        NAMES                               atn-application-entity
        WITH ATTRIBUTES                     { commonName }
        ID                                  id-nf-atnApplEntityNameForm }
    atnAmhsDLNameForm                 NAME-FORM  ::=  {
        NAMES                     atn-amhs-distribution-~~L~~list
        WITH ATTRIBUTES           { commonName }
        ID                        id-nf-atnAmhsDLNameForm }

    atnAmhsUANameForm                 NAME-FORM  ::=  {
        NAMES                     atn-amhs-useragent
        WITH ATTRIBUTES           { commonName }
        ID                        id-nf-atnAmhsUANameForm }

    atnAmhsGatewayNameForm            NAME-FORM  ::=  {
        NAMES                     atn-amhs-gateway
        WITH ATTRIBUTES           { commonName }
        ID                        id-nf-atnAmhsGatewayNameForm }

    atnAmhsMDNameForm                 NAME-FORM  ::=  {
        NAMES                     atn-amhsMD
        WITH ATTRIBUTES           { commonName }
        ID                        id-nf-atnAmhsMDNameForm }

    atnOrgNameForm                    NAME-FORM  ::=  {
        NAMES                     atn-organization
        WITH ATTRIBUTES           { ~~O~~organizationName }
        ID                        id-nf-atnOrgNameForm }

    atnAircraftNameForm               NAME-FORM  ::=  {
        NAMES                     atn-aircraft
        WITH ATTRIBUTES           {atn-aircraftIDName }
        ID                        id-nf-atnAircraftNameForm }

    atnFacilityNameForm                     NAME-FORM  ::=  {
        NAMES                     atn-facility
        WITH ATTRIBUTES           {atn-facility-name }
        ID                        id-nf-atnFacilityNameForm }

    atnIdrpRouterNameForm             NAME-FORM  ::=  {
        NAMES                     atn-idrp-router
        WITH ATTRIBUTES           {commonName }
        ID                        id-nf-atnIdrpRouterNameForm }

    atnDSANameForm                    NAME-FORM  ::=  {
        NAMES                     atn-dSA
        WITH ATTRIBUTES           {commonName }
        ID                        id-nf-atnDSANameForm }

END     -- of ATN schema object classes and attribute type definitions
```

2.4.11 Reference definition of object identifiers for ATN directory schema

```
ATNDirectoryObjectIdentifiers { iso(1) identified-organisation(3) icao(27) atn(0) objectIdentifiers(0) atnDirectory(0) }

-- Note — this is the definitive register of all schema object identifiers for atn-specific object
-- classes, atn-specific attributes and atn-specific name forms.

DEFINITIONS AUTOMATIC TAGS ::=

BEGIN

--              EXPORTS EVERYTHING

ATN Directory Schema

-- Note — the following sets atn-specific directory object classes high order
-- identification to 'id-oc'

id-oc OBJECT IDENTIFIER ::= { iso(1) identified-organisation(3) icao(27) atn-directory(7) oc 0}

-- Note — the following sets atn-specific directory object classes high order
-- identification to 'id-at'

id-at OBJECT IDENTIFIER ::=  { iso(1) identified-organisation(3) icao(27) atn-directory(7) at 1}

-- Note — the following sets atn-specific name forms high order
-- identification to 'id-nf'

id-nf OBJECT IDENTIFIER ::=  { iso(1) identified-organisation(3) icao(27) atn-directory(7) nf 2}

-- definition of directory object class object identifiers

id-oc-atn-AmhsUser OBJECT IDENTIFIER ::=                       {id-oc 1 }
id-oc-atn-OrganisationalUnit OBJECT IDENTIFIER ::=             {id-oc 2}

id-oc-atn-OrganizationalPerson OBJECT IDENTIFIER ::=           {id-oc 3}

id-oc-atn-OrganizationalRole OBJECT IDENTIFIER ::=             {id-oc 4}

id-oc-atn-ApplicationEntity OBJECT IDENTIFIER ::=              {id-oc 5}

id-oc-atn-CertificationAuthority OBJECT IDENTIFIER ::=         {id-oc 6}

id-oc-atn-AmhsDistributionList OBJECT IDENTIFIER ::=           {id-oc 7}

id-oc-atn-AmhsUserAgent OBJECT IDENTIFIER ::=                  {id-oc 8}

id-oc-atn-AmhsGateway OBJECT IDENTIFIER ::=                    {id-oc 9}

id-oc-atn-Aircraft OBJECT IDENTIFIER ::=                       {id-oc 10}

id-oc-atn-AtnFacility OBJECT IDENTIFIER ::=                    {id-oc 11}

id-oc-atn-amhsMD OBJECT IDENTIFIER ::=                         {id-oc 12}
```

```
id-oc-atn-idrpRouter OBJECT IDENTIFIER ::=                      {id-oc 13}

id-oc-atn-AtnDirectorySystemAgent OBJECT IDENTIFIER ::=         {id-oc 14}

id-oc-atn-Atn-Organization OBJECT IDENTIFIER ::=                {id-oc 15}

-- definition of atn-specific attribute type object identifier values

id-at-atn-AF-address OBJECT IDENTIFIER ::=                      {id-at 1}

id-at-atn-PerCertificate OBJECT IDENTIFIER ::=                  {id-at 2}

id-at-atn-DerCertificate OBJECT IDENTIFIER ::=                  {id-at 3}

id-at-atn-amhs-direct-access OBJECT IDENTIFIER ::=              {id-at 4}

id-at-atn-facilityName OBJECT IDENTIFIER ::=                    {id-at 5}

id-at-atn-aircraftIDName OBJECT IDENTIFIER ::=                  {id-at 6}

id-at-atn-Version OBJECT IDENTIFIER ::=                         {id-at 7}

id-at-~~-~~atn-ipm-heading-extensions OBJECT IDENTIFIER ::=            {id-at 8}

id-at-atn-amhs-global-domain-identifier OBJECT IDENTIFIER ::=   {id-at 9}

id-at-atn-icao-designator OBJECT IDENTIFIER ::=                 {id-at 10}

id-at-atn-Net OBJECT IDENTIFIER ::=                             {id-at 11}

id-at-atn-Amhs-addressing-scheme OBJECT IDENTIFIER ::=          {id-at 12}

id-at-atn-AmhsMD-naming-context OBJECT IDENTIFIER ::=           {id-at 13}

id-at-atn-maximum-number-of-body-parts OBJECT IDENTIFIER ::=    {id-at 14}

id-at-atn-maximum-text-size OBJECT IDENTIFIER ::=               {id-at 15}

id-at-atn-maximum-file-size OBJECT IDENTIFIER ::=               {id-at 16}

id-at-atn-use-of-amhs-security OBJECT IDENTIFIER ::=            {id-at 17}

id-at-atn-use-of-directory OBJECT IDENTIFIER ::=                {id-at 18}

id-at-atn-group-of-addresses OBJECT IDENTIFIER ::=              {id-at 19}

-- Name form registrations

id-nf-atnOrgUnitNameForm ::=                                    {id-nf 0}

id-nf-atnOrgPersonNameForm ::=                                  {id-nf 1}
```

```
id-nf-atnOrgRoleNameForm ::=                         {id-nf 2}

id-nf- atnApplEntityNameForm ::=                     {id-nf 3}

id-nf-atnAmhsDLNameForm ::=                          {id-nf 4}

id-nf-atnAmhsUANameForm::=                           {id-nf 5}

id-nf-atnAmhsGatewayNameForm::=                      {id-nf 6}

id-nf-atnAmhsMDNameForm::=                           {id-nf 7}

id-nf-atnOrgNameForm::=                              {id-nf 8}

id-nf-atnAircraftNameForm ::=                        {id-nf 9}

id-nf-atnFacilityNameForm ::=                        {id-nf 10}

id-nf-atnIdrpRouterNameForm ::=                      {id-nf 11}

id-nf-atnDSANameForm ::=                             {id-nf 12}

END        --  of atn directory schema object identifiers and attribute syntaxes
```

~~**Chapter 5**~~

2.5 ATN DIRECTORY PROTOCOLS

Formatted: Normal, Centered

Formatted: Font: Bold, Complex Script Font: Bold

2.5.1 Security

2.5.1.1~~.1~~ Security in ATN directory protocols is specified as a single overall optional functional group [StrongSec], based on specifications in this manual and provides strong security protection for the DIB content. This functional group may or may not be implemented in a conformant implementation.

2.5.1.2 Authentication

Formatted: Font: Italic

Formatted: Left

2.5.1.2.1 DSAs and DUAs implementing the [StrongSec] functional group shall support strong authentication.

2.5.1.2.2 The supporting cryptographic processing to produce values for strong authentication interchanges need to be established as appropriate within the operational domain or by bilateral agreement.

2.5.1.2.3 This does not preclude additional local security measures to be taken for protection of the DIB contents integrity. Such measures are out of the scope of this manual.

2.5.1.3 Signature generation

Formatted: Font: Italic

Formatted: Left

2.5.1.3.1 DSAs and DUAs required to implement strong security [StrongSec] for signature generation shall implement the security processing specified in Chapter 3.~~Doc 9705 Sub-Volume VIII section 8.3.1.8.2 / Doc 9880 Part IV.~~

2.5.1.4 Signature verification

Formatted: Font: Italic

Formatted: Left

2.5.1.4.1 DSAs and DUAs required to implement strong security [StrongSec] for signature verification shall implement the security processing specified in Chapter 3.~~Doc 9705 Sub-Volume VIII, section 8.3.1.8.3 / Doc 9880 Part IV.~~

2.5.1.5 Certificate validation

Formatted: Font: Italic

Formatted: Left

2.5.1.5.1 DSAs and DUAs required to implement strong security [StrongSec] for certificate validation shall validate the operation or response originator's certificate as specified in ~~this manual~~Chapter 3.

2.5.1.6 Identification of the ATN digital signature scheme

Formatted: Font: Italic

Formatted: Left

2.5.1.6.1 DSAs and DUAs required to implement strong security [StrongSec] shall identify the use of the ATN digital signature scheme as specified in ~~this manual~~Chapter 3.

Note.— Chapter 3 is under development, and the provisions above may need to be refined when it is completed.

2.5.2 Support of directory access protocol DAP

2.5.2.1 DUA conformance to DAP

Formatted: Font: Italic

Formatted: Left

2.5.2.1.1 The use of the DAP by a DUA which invokes an operation on a DSA and receives a response or an error is specified in ISO/IEC 9594. This section further refines this specification by constraining the use of DAP to the requirements of the ATN.

2.5.2.1.2 A DUA shall conform to all mandatory requirements specified in the PRL Tables of ISO/IEC 13248-1 | ITU-T Rec. X.583.

2.5.2.1.3 A DUA shall additionally support all the elements specified as options in ISO/IEC 13248-1 | ITU-T Rec. X.583 that are listed in Table 2-18~~5-1~~ depending on the type of the DUA specified.

2.5.2.1.4 A DUA shall conform to all dynamic requirements of ISO/IEC 9594-5:1995 | ITU-T Rec. X.519:1993 and all the requirements in this manual.

2.5.2.1.5 A DUA shall accept any protocol conformant response to each operation it supports, including responses containing protocol elements which are unknown or not supported by the DUA. For this purpose, to accept a response means to receive the response without taking the actions associated with the standards with protocol errors, including presentation, ROSE and DAP errors.

2.5.2.1.6 A DUA should limit its APDU size to less than 1 Mb octets. A DUA may send an APDU of any size, but since the DSA is not required to process APDUs over 1 Mb octets in length, a DAP error may result for APDUs greater than that size.

2.5.2.1.7 If the abandon operation is not supported, all operation requests shall include a non-zero timeLimit.

2.5.2.1.8 The DirectoryAccessAC application context shall be supported.

2.5.2.1.9 If the DUA supports abandon operations, it shall support the asynchronous (ROSE class 2) mode of operation.

2.5.2.1.10 A DUA shall support the rules of extensibility as defined in Section 7.5.1 of ISO/IEC 9594-5.

Bind response

2.5.2.1.11 The operation of DAP is through interactions between the DUA and the DSA. The first action in an instance of communication is a bind request to which the response is a bind response. This section deals with the processing of a bind response by the DUA.

2.5.2.1.12 The specification of DUA responses to a bind request with security parameters is contained in this section.

2.5.2.1.13 When a bind with no credentials is issued, a DUA shall be capable of accepting a BindResponse with no credentials and of ignoring any credentials in the BindResponse.

2.5.2.1.14 When a bind with simple credentials of any form is issued, unsupported protocol elements in the BindResponse shall be ignored.
2.5.2.1.15 A DUA shall be permitted, but not required, to accept a BindResponse in which the type of credentials (simple, strong or externalProcedure) in the BindResponse is a different response from that in the bind.

2.5.2.1.16 To terminate an association due to rejection of the credentials in the BindResult, a DUA shall invoke an unbind operation.

2.5.2.2 DSA conformance to DAP

Formatted: Font: Italic

Formatted: Left

2.5.2.2.1 ISO/IEC 9594 defines the behaviour of a DSA regarding the operation of the DAP for communicating with a DUA. It covers the DSA performing the responder role of DAP, receiving the invocation of an operation from a DUA, and responding with a result or error response. This section defines the capabilities and constraints on support for DAP by DSAs so that DUAs are able to interwork with the directory service.

2.5.2.2.2 A DSA implementation shall conform to all requirements of Clause 9.2 of ISO/IEC 9594-5:1995 | ITU-T Rec. X.519:1993 applicable to a DSA implementing the DirectoryAccessAC application context, including any requirements directly and indirectly referenced by that clause.

2.5.2.2.3 DSAs shall conform to all requirements specified in the PRL tables of ISO/IEC 13248-1.

2.5.2.2.4 DSAs shall support all the options listed in Table 7.6.1 — 1 according to the type of DUA specified. A DSA shall conform to all dynamic requirements of ISO/IEC 9594-5:1995 | ITU-T Rec. X.519:1993 and all the requirements in this part of Doc 9880.

2.5.2.2.5 When an oversize request APDU is received or an oversize response APDU would be sent, it shall be valid to discard it.

2.5.2.2.6 If an oversize APDU is discarded, the appropriate error (i.e. the service error “unwillingToPerform” or “administrativeLimitExceeded”) should be returned. A DSA may be operated with administrative limits on an APDU size lower than those specified in the static conformance requirements. The possible effects on distributed operations should be considered in establishing such limits. ISO/IEC 9594 does not impose constraints on the actions of the supporting layers upon receiving APDUs in excess of the limits specified.

Filter constraints

2.5.2.2.7 Each DSA shall support at least 32 FilterItems in a SearchArgument.

Filter nesting

2.5.2.2.8 Each DSA shall support the nesting of at least eight levels deep for any possible combination of elements of the filter (i.e. choice of item, and or, and not). An implementation may constrain the deepest of the eight levels to be an item.

Exceeding filter constraints

2.5.2.2.9 When a request exceeding the filter constraints is received, the DSA may refuse to perform the request if the DSA reaches the operation evaluation phase, in which case the serviceError response shall be ServiceProblem, unwillingToPerform.

Search strings support

2.5.2.2.10 A DSA shall support search strings (“initial”, “any” or “final” elements) of at least 1 024 characters.

Note.— For approximate matching, a DSA is not required to use any matching rule other than the relevant equality matching rule.

2.5.2.2.11 A DSA shall support the performer role.

2.5.2.2.12 The directory Accesswatch application context shall be supported.

2.5.3 DAP PRL

2.5.3.1 In addition to conformance with the PRLs in ISO/IEC 13248-1 | ITU-T Rec. X.583, implementations of DSAs and the three types of DUA shall support the protocol elements indicated for the implementation type indicated in Table 2-18~~5-1~~.

2.5.3.2 The base standard PRLs are specified in ISO/IEC 13248-1 | ITU-T Rec. X.583. The following PRL identifies where elements classified as optional in ISO/IEC 13248-1, Annex A are re-classified to mandatory or conditional for the ATN support of DAP. They are therefore “delta” requirements. There is an implicit assumption that all the mandated requirements of the base standard are inherited, and the requirements of the table are additional requirements of the ATN directory.

Table 2-18~~5-1~~. DUA and DSA options for the ATN directory DAP

Ref. no.	*Protocol element and operation*	*Administrative DUA*	*Autonomous operational DUA*	*Operational personnel DUA*	*DSA*	*ISO/IEC 13248-1 | ITU-T Rec. X.583 ref.*
	Operations					A.6.3.2.1

Ref. no.	*Protocol element and operation*	*Administrative DUA*	*Autonomous operational DUA*	*Operational personnel DUA*	*DSA*	*ISO/IEC 13248-1 | ITU-T Rec. X.583 ref.*
1	Bind	M	M	M	M	"
2	Unbind	M	M	M	M	"
3	Read	M	M	M	M	"
4	Compare	M	M	M	M	"
5	List	M	X	M	M	"
6	Search	M	M	M	M	"
7	Add Entry	M	X	X	M	"
8	Remove Entry	M	X	X	M	"
9	Modify entry	M	X	X	M	"
10	Modify DN	M	X	X	M	"
11	General capabilities and extensions					A.6.2.1.1, A.6.2.2.1 and A.6.3.2.2
12	Support of signed operations	C1	C1	C1	C1	"
13	modifyRightsRequest	M	X	X	M	"
14	pagedResultsRequest	M	X	M	M	"
15	newSuperior	M	X	X	M	"
	Strong authentication and signed operations					
16	Strong authentication for the DAP bind operation in both initiator role and responder role	C1	C1	C1	C1 (Responder role only)	"
17	Strong authentication for the DAP bind result in both initiator role and responder role	C1	C1	C1	C1 (Responder role only)	"
18	Signed read operation and signed read result	C1	C1	C1	C1	"
19	Signed compare operation and signed compare result	C1	C1	C1	C1	"
20	Signed list operation and signed list result	C1	X	C1	C1	"
21	Signed search operation and signed search result	C1	C1	C1	C1	"

Ref. no.	*Protocol element and operation*	*Administrative DUA*	*Autonomous operational DUA*	*Operational personnel DUA*	*DSA*	*ISO/IEC 13248-1 | ITU-T Rec. X.583 ref.*
22	Signed add entry operation and signed add entry result	C1	X	X	C1	“
23	Signed remove entry operation and signed remove entry result	C1	X	X	C1	“
24	Signed modify entry operation and signed modify entry result	C1	X	X	C1	“
25	Signed modify DN operation and signed modify DN result	C1	X	X	C1	“
26	Support for the distinguished encoding rules	C1	C1	C1	C1	“
27	Support for certificate version 3	C1	C1	C1	C1	“
28	Support for certificate revocation list version 3	C1	C1	C1	C1	“
29	Support for authority revocation list version 3	C1	C1	C1	C1	“
	OPERATION PROTOCOL ELEMENTS					
30	Read operation	M	M	M	M	A.6.3.3.3
31	Modify rights request and results for:	M	X	X	M	“
32	-Entry	M	X	X	M	“
33	-Attribute	M	X	X	M	“
34	-Value	M	X	X	M	“
35	-Permission	M	X	X	M	“
36	List operation	M	X	M	M	A.6.3.3.6
37	Paged results	M	X	M	M	
38	Name	M	X	O	M	
39	Aliasentry	M	X	O	M	
40	FromEntry	M	X	O	M	
41	QueryReference	M	X	M	M	
42	UncorrellatedListInformation	M	X	M	M	
43	partialOutcomeQualifier	M	X	M	M	
44	Compare operation	M	M	M	M	A.6.3.3.4
45	name	M	O	O	M	

Ref. no.	*Protocol element and operation*	*Administrative DUA*	*Autonomous operational DUA*	*Operational personnel DUA*	*DSA*	*ISO/IEC 13248-1 | ITU-T Rec. X.583 ref.*
46	fromEntry	M	O	O	M	
47	matchedSubtype	M	O	O	M	
48	Search Operation	M	M	M	M	A.6.3.3.7
49	Subset	M	M	O	M	
50	SearchAliases	M	M	O	M	
51	PagedResults	M	X	M	M	
52	QueryReference	M	X	M	M	
53	UncorrellatedsearchInfo	M	M	M	M	
54	partialoutcomeQualifier	M	X	M	M	
55	Modify DN operation	M	X	X	M	A.6.3.3.11
56	NewSuperior	M	X	X	M	
57	Errors and parameters	M	M	M	M	A.6.3.3.12
58	invalidSignature	C1	C1	C1	C1	
59	protectionRequired	C1	C1	C1	C1	
60	invalidQueryReference	C2	X	C2	C2	
61	DUA common arguments elements	M	M	M	M	A.6.3.3.13
62	operationProgress	M	O	O	M	
63	referenceType	M	O	O	M	
64	entryOnly	M	O	O	M	
65	exclusions	M	O	O	M	
66	nameResolveOnMaster	M	O	O	M	
67	DUA common results elements	M	M	M	M	A.6.3.3.14
68	aliasDereferenced	M	M	M	M	
69	DUA Servicecontrol elements	M	M	M	M	A.6.3.3.15
70	Attributesizelimit	M	O	O	M	
71	DUA entry information selection	M	M	M	M	A.6.3.3.16
72	Attributes	M	M	M	M	
73	AllUserAttributes	M	M	M	M	
74	Select	M	M	M	M	
75	Entry information elements	M	M	M	M	A.6.3.3.17

Ref. no.	*Protocol element and operation*	*Administrative DUA*	*Autonomous operational DUA*	*Operational personnel DUA*	*DSA*	*ISO/IEC 13248-1 | ITU-T Rec. X.583 ref.*
76	FromEntry	M	M	M	M	
77	Information	M	M	M	M	
78	AttributeType	M	M	M	M	
79	Attribute	M	M	M	M	
80	NonCompleteEntry	M	M	M	M	
81	Filter item elements	M	M	M	M	A.6.3.18
82	Equality	M	M	M		
83	ExtensibleMatch	M	O	O	M	
84	Paged results elements	M	X	M	M	
85	NewRequest	M	X	M	M	
86	QueryReference	M	X	M	M	
87	Continuation reference elements	M	M	M	M	A.6.3.3.21
88	NextRDNtobeResolved	M	M	M	M	
89	RDNsResolved	M	M	M	M	
90	EntryOnly	M	M	M	M	
91	ReturntoDUA	M	M	M	M	
92	NameResolveonMaster	M	M	M	M	
93	Supported references	M	M	M	M	A.6.3.3.25
94	SelfReference	M	M	M	M	
95	Superior reference	M	M	M	M	
96	ImmediateSuperiorReference	M	M	M	M	
97	SubordinateReference	M	M	M	M	
98	Non-specific SubordinateReference	M	M	M	M	
99	Cross reference	M	M	M	M	
	SECURITY					
100	DUA authentication – DAP initiator	M	M	M	M	A.6.3.1.1
101	Simple	M	M	M	M	
102	Strong authentication	C1	C1	C1	C1	
103	Strong	C1	C1	C1	C1	
104	Two way bind request	C1	C1	C1	C1	

Ref. no.	*Protocol element and operation*	*Administrative DUA*	*Autonomous operational DUA*	*Operational personnel DUA*	*DSA*	*ISO/IEC 13248-1 | ITU-T Rec. X.583 ref.*
105	Strong authentication – initiator	C1	C1	C1	-	
106	Strong authentication – responder	-	-	-	C1	
107	Common algorithms	C1	C1	C1	C1	
108	Generation of certification path	C1	C1	C1	C1	
109	DUA bind elements	M	M	M	M	A.6.3.3.1.1
110	Time1	C1	C1	C1	C1	
111	Random1	C1	C1	C1	C1	
112	CertificationPath	C1	C1	C1	C1	
113	Name	C1	C1	C1	C1	
114	DUA bind result elements	M	M	M	M	A.6.3.3.1.2
115	Time1	C1	C1	C1	C1	
116	Random1	C1	C1	C1	C1	
117	CertificationPath	C1	C1	C1	C1	
118	Name	C1	C1	C1	C1	

C1 – if [strongsec] then M else O.
C2 – If Pagerequest is required then M else O.

Note.— The table implies that a DSA supports the superset of all elements supported by all DUAs accessing the DSA.

2.5.4 DSA support for the DSP

2.5.4.1 DSA support of distributed operations

Formatted: Font: Italic

Formatted: Left

2.5.4.1.1 The use of the DSP by a DSA that invokes an operation on a DSA and receives a response or an error is specified in ISO/IEC 9594-5. This section further refines the specification in the ISP by constraining the use of DSP to the requirements of the ATN.

2.5.4.1.2 A DSA shall conform to all requirements mandated in the PRL tables of ISO/IEC 13248-2.

2.5.4.1.3 In addition to 2.5.4.1.2, a DSA shall support all the requirements expressed in Table 2-19~~5-2~~.

2.5.4.1.4 A DSA shall conform to all dynamic requirements of ISO/IEC 9594-5:1995 (ITU-T Rec. X.519:1993) and all the requirements in this manual.

2.5.4.1.5 A DSA supporting chained operations shall support the invoker role.

2.5.4.1.6 A DSA shall be able to use the referral mode of interaction, even if it only supports the DirectorySystemAC application context.

2.5.4.1.7 A DSA shall be capable of handling APDUs of at least 1Mb.

2.5.4.1.8 DSAs shall conform to the dynamic requirements as specified in Section 9.2.3 of ISO/IEC 9594-5.

2.5.4.1.9 DSAs shall conform to the error handling requirements as specified in Sections 7.4.1 and 7.5 of ISO/IEC 9594-5.

2.5.4.1.10 DSAs should use A-ABORT to disconnect from other DSAs. Either the initiating or the responding DSA is permitted to initiate an unbind. However, a DSA that has initiated an unbind may be unable to handle subsequently received returns from the responding DSA that were emitted prior to the unbind response; in view of this uncertainty, the use of A-ABORT is clearer.

2.5.4.1.11 DSAs shall conform to the requirements specified in ISO/IEC 9594-2 for knowledge references and root context.

2.5.4.1.12 A DSA should support the ‘First Level DSA’ DIT structure as described in ISO/IEC 9594-2, Section 22.5. This is because the DIT structure will be relatively flat at the top levels of the hierarchy.

2.5.4.1.13 DSAs shall conform to the requirements specified in ISO/IEC 9594 for administrative authorities.

2.5.4.1.14 DSAs shall conform to the requirements specified in ISO/IEC 9594 for operations requirements.

2.5.5 DSA support for DISP

2.5.5.1 Use of DISP

Formatted: Font: Italic

Formatted: Left

2.5.5.1.1 If a DSA is required to share DIB Information with other DSAs for DIB replication, it shall support the DISP as specified in ISO/IEC 9594-5, Clause 6.5.

Table 2-19~~5-2~~. DSP requirements list

Ref. no	*Protocol element and operation*	*ATN DSA*	*Reference*	*Notes*
	Reference types			
1	Superior	M		
2	Subordinate	M		
3	CrossReference	M		
4	Non-specific subordinate reference	O		
5	Immediate superior reference	M		
	DSA bind arguments			
6	Credentials	M	X.584	
7	Simple	M	X.584	
8	Validity	C2	X.584	
9	Time 1	C2	ISO/IEC 9594-1995	
10	Random 1	C2	“	
11	Password	M		
12	Unprotected	M		
13	protected	C2		
14	Strong	C1		
15	Name	C1		“
16	Certification path	C1		
	Signed-chained operations		ISO/IEC 9594 — 1995	
17	Signed-chained read	C1	“	
18	Signed-chained compare	C1	“	
19	Signed-chained list	C1	“	
20	Signed-chained search	C1	“	
21	Signed-chained AddEntry	O	“	
22	Signed-chained RemoveEntry	O	“	
23	Signed-chained ModifyEntry	O	“	
24	Signed-chained modify DN	O	“	
	Chained arguments elements		“	
25	Security parameters	C1	“	
26	Unique identifier	C1	“	
27	Authentication level	C1	“	
	Chained result elements			
28	SecurityParameters	C1	“	

C1: If [StrongSec] then M else O.
C2 : If Pagerequest is required then M else O.

2.5.5.2 DSA DISP knowledge references

Formatted: Font: Italic

Formatted: Left

2.5.5.2.1 A DSA supporting DISP shall support supplier references and master references.

2.5.5.3 Use of signed operations for DISP

Formatted: Font: Italic

Formatted: Left

2.5.5.3.1 If a DSA supports the DISP, then it shall protect the transferred DIB information using the strong security functional group [StrongSec] for all operations, or it shall use other equivalent security measures to prevent information corruption and masquerade.

2.5.6 Support for DOP

2.5.6.1 The DOP is not profiled in this manual.

2.5.7 Use of ATN application service elements, presentation session and transport services

2.5.7.1 Use of ROSE services

Formatted: Font: Italic

Formatted: Left

2.5.7.1.1 The use of ROSE by ATN DUAs and DSAs shall be as specified in ISO/IEC 9594-5, Section 6.7.1.

2.5.7.1.2 The ROSE is defined in ITU-T Rec. X.881 | ISO 9072-2.

2.5.7.2 Use of RTSE services

Formatted: Font: Italic

Formatted: Left

2.5.7.2.1 The use of RTSE by ATN DSAs in support of DISP, if implemented, shall be as specified in ISO/IEC 9594-5, Section 6.7.2.

2.5.7.2.2 The RTSE is defined in ITU-T Rec. X.218 | ISO/IEC 9066-1.

2.5.7.2.3 The RTSE provides for the reliable transfer of APDUs. The RTSE ensures that each APDU is completely transferred exactly once or that the sender is warned of an exception. The RTSE recovers from communication and end-system failure and minimizes the amount of retransmission needed for recovery.

2.5.7.2.4 Alternative application contexts with and without RTSE are defined to support the DISP.

2.5.7.3 Use of ACSE services

Formatted: Font: Italic

Formatted: Left

2.5.7.3.1 The use of ACSE by ATN DUAs and DSAs shall be as specified in ISO/IEC 9594-5, Section 6.7.3.

2.5.7.3.2 The ACSE is defined in CCITT Rec. X.217 | ISO 8649.

2.5.7.3.3 The ACSE provides for the control (establishment, release and abort) of application-associations between AEs.

2.5.7.4 Use of the presentation service

Formatted: Font: Italic

Formatted: Left

2.5.7.4.1 The use of the presentation service by ATN DUAs and DSAs shall be as specified in ISO/IEC 9594-5, Section 6.7.4.

2.5.7.4.2 The presentation service is defined in ITU-T Rec. X.216 | ISO/IEC 8822.

2.5.7.4.3 The presentation layer coordinates the representation (syntax) of the application layer semantics that are to be exchanged.

2.5.7.4.4 In normal mode, a different presentation-context is used for each abstract-syntax included in the application-context.

2.5.7.5 Use of the session service

Formatted: Font: Italic

Formatted: Left

2.5.7.5.1 The use of the connection-oriented session service as required by the presentation protocol shall be supported.

2.5.7.6 Use of transport service and mapping to underlying services

Formatted: Font: Italic

Formatted: Left

2.5.7.6.1 ATN directory protocols shall make use of the connection mode transport service in either or both of the following configurations:

a) provided by the ATN ICS as generally specified in Part III with the additional provisions in 2.5.7.6.2 to 2.5.7.6.5; or

b) provided by the IPS as specified in the *Manual on the Aeronautical Telecommunication Network (ATN) using Internet Protocol Suite (IPS) Standards and Protocols* (Doc 9896) with the additional provisions in 2.5.7.6.6 to 2.5.7.6.8.

Transport service over the ATN ICS

2.5.7.6.2 The use of the connection-oriented transport service provided by the ATN internet shall be as specified in Clause 6 of ISO/IEC 8327-1 except as noted in this section.

2.5.7.6.3 The transport service user shall indicate in all T-CONNECT requests that the transport expedited flow is not required.

2.5.7.6.4 The ATN DIR does not set the ATN security label and provides a transport layer interface that is compliant with commercial software systems.

2.5.7.6.5 This means that DIR traffic is carried as general communications.

Transport service over the IPS

2.5.7.6.6 For the support of the ATN DIR over the IPS, the connection mode transport service provided by the IPS TCP shall be used.

2.5.7.6.7 When IPv4 is used, the connection mode transport service over the TCP shall be provided as specified in RFC1006.

2.5.7.6.8 When IPv6 is used, the connection mode transport service over the TCP shall be provided as specified in RFC2126.

THIS PAGE LEFT BLANK INTENTIONALLY

Chapter 3

SECURITY

(Under development by update of Doc 9705 Sub-Volume VIII)

THIS PAGE LEFT BLANK INTENTIONALLY

Chapter 4

IDENTIFIER REGISTRATION

4.1 INTRODUCTION

4.1.1 Overview

4.1.1.1 The ATN Identifier Registration acts as a central repository for common identifiers used in the ATN. This includes object identifiers (OIDs), application identifiers and other common identifier information.

4.1.1.2 OIDs are used to name information objects, such as application contexts, abstract syntaxes and ASN.1 modules within an OSI application protocol specification. For the ATN applications, this includes the objects contained in the various Parts of Doc 9880-AN/466. In order to ensure that successive applications do not have OID conflicts within the ATN domain, all of the ATN-specific OIDs are specified in this document. Other OIDs which are local to the various Parts (either OSI standard or ATN defined) are not specified here; they are referenced and/or defined as applicable by the Part that uses them. OIDs which are used by two or more Parts may be specified here.

4.1.1.3 Application identifiers are ATN applications' AE Qualifiers. These are assigned to individual applications as operational needs are identified and the applications themselves are developed.

4.2 ATN IDENTIFIERS

4.2.1 Application level naming and context definition

4.2.1.1 ATN Naming Hierarchy

4.2.1.1.1 Names, in the form of object identifiers (OIDs), are assigned here to the defined ATN entities.

4.2.1.1.2 ISO/IEC 9834-1 | ITU-T Rec. X.660 Amd. 2 specifies the top of the hierarchical OID name space. At the first level, provision is made for ISO, International Telecommunication Union - Telecommunication Standardisation Sector (ITU-T) and joint ISO/ITU-T sub-name spaces. The ISO name space is further subdivided into:

a) standard (0)

b) registration-authority (1)

c) member-body (2)

d) identified-organisation (3)

4.2.1.1.3 ICAO has requested and obtained the allocation of an International Code Designator (ICD), according to ISO 6523. The ICD obtained, name and number “icao (27)”, uniquely identifies ICAO and allows ICAO to establish its own object identifier name space within the International Organisation arc using the prefix: { iso (1) identified-organisation (3) icao (27) }.

4.2.1.1.4 Within the ICAO name space, the initial allocation of object identifiers shall follow the structure and values defined here.

4.2.1.1.5 In the future, it is likely that the ATN object identifier tree will have further levels of structure, and that fully location-independent values will be assigned.

4.2.1.1.6 The ATN naming hierarchy is illustrated in Figure 4-1.

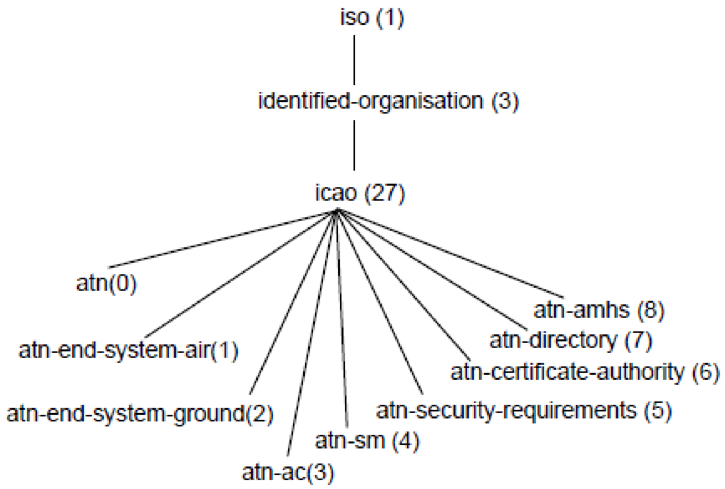

Figure 4-1. ATN Naming Hierarchy

4.2.1.1.7 Immediately under the ICAO arc, the values specified in Table 4-1 shall be used to specify the next level of the naming hierarchy.

Table 4-1. Top-level ICAO Identifiers

Name and numeric value	*Description*
atn (0)	General ATN identifiers
atn-end-system-air (1)	ATN aircraft end systems. The subsequent OID components beneath are defined in Part III
atn-end-system-ground (2)	ATN ground end systems. The subsequent OID components beneath this arc are defined in Part III
atn-ac (3)	ATN application context names. The subsequent OID components beneath this arc are defined in Part III
atn-sm (4)	RESERVED
atn-security-requirements (5)	ATN security. The subsequent OID components beneath this arc are defined in section 4.2.1.3 and in Chapter 3
atn-certificate-authority (6)	ATN certificate authority. The subsequent OID components beneath this arc are defined in Chapter 3
atn-directory (7)	ATN Directory. The subsequent OID components beneath this arc are defined in Chapter 2
atn-amhs (8)	ATN AMHS application. The subsequent OID components beneath this arc are defined in Part II

4.2.1.2 Application types

4.2.1.2.1 In the Application Process title (as defined in Part III) that identifies each ATN application process type, there is an <app-type> element. Table 4-2 will serve as a global register for all standard ATN application types. Additionally, Table 4-2 may be used to identify application types, for example in the Context Management application CM-logon service.

4.2.1.2.2 The app-type arc of the Application Process title object identifier represents the ATN application type (e.g. “ADS-C” or “CMA”), and shall take one of the values specified in Table 4-2.

Table 4-2. Assigned app-types and values

ATN ASE type	*ATN app-type name and numeric value*
Automatic Dependent Surveillance (Contract Mode)	ADS-C (0)
Context Management Application	CMA (1)
RESERVED	(2)
RESERVED	(3)

Formatted Table

ATN ASE type	*ATN app-type name and numeric value*
RESERVED	(4)
RESERVED	(5)
RESERVED	(6)
ATS Message Application	AMS (7)
AFTN-AMHS Gateway	GWB (8)
ATS Message User Agent	AUA (9)
ADS Report Forwarding	ARF (10)
RESERVED	(11)
RESERVED	(12)
RESERVED	(13)
Controller Pilot Data Link Communication	CPC (22)

Formatted Table

4.2.1.3 ATN Object Identifiers ASN.1

```
ATNObjectIdentifiers { iso(1) identified-organization(3) icao(27) atn(0) objectIdentifiers(0) }
DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

-- EXPORTS everything

icao-arc        OBJECT IDENTIFIER ::= { iso(1) identified-organization(3) icao(27) }

-- Root of the ICAO OBJECT IDENTIFIER space

icao-atn        OBJECT IDENTIFIER ::= { icao-arc atn(0) }

-- General ATN

icao-atn-end-system-air
                OBJECT IDENTIFIER ::= { icao-arc atn-end-system-air(1) }

-- ATN aircraft end system

icao-atn-end-system-ground
                OBJECT IDENTIFIER ::= { icao-arc atn-end-system-ground(2) }

-- ATN ground end system

icao-atn-ac     OBJECT IDENTIFIER ::= { icao-arc atn-ac(3) }

-- ATN application context names
```

```
icao-atn-sm   OBJECT IDENTIFIER ::= { icao-arc atn-sm(4) }

-- ATN system management

icao-atn-security-requirements
              OBJECT IDENTIFIER ::= { icao-arc atn-security-requirements(5) }

-- ATN security

icao-atn-certificate-authority
              OBJECT IDENTIFIER ::= { icao-arc atn-certificate-authority(6) }

-- ATN certificate authority

icao-atn-directory
              OBJECT IDENTIFIER ::= { icao-arc atn-directory(7) }

-- ATN Directory

icao-atn-amhs
              OBJECT IDENTIFIER ::= { icao-arc atn-amhs(8) }

-- ATN AMHS

--
-- ATN security OIDs shared between Parts III and IV
--
secids        OBJECT IDENTIFIER ::= { icao-atn-security-requirements }

-- Categories of information object --
modules       OBJECT IDENTIFIER ::= { secids 1 }

-- Security ASN.1 modules in Part III --
securityExchanges     OBJECT IDENTIFIER ::= { modules 1 }
abstractSyntax    OBJECT IDENTIFIER ::= { modules 2 }

-- Security ASN.1 module in Part IV --
atnPKI        OBJECT IDENTIFIER ::= { modules 3 }


END -- ATN OID definitions
```

— END —