



ICAO

Doc 9880

Technical Specifications for ATN using ISO/OSI Standards and Protocols

Second edition, 2016

Part IV – Directory Services, Security and Identifier Registration



Approved by and published under the authority of the Secretary General

INTERNATIONAL CIVIL AVIATION ORGANIZATION **Documents**



Document Sharing Hub

Doc 9880
AN/466



Manual on Detailed Technical Specifications for the Aeronautical Telecommunication Network (ATN) using ISO/OSI Standards and Protocols

**Part IV — Directory Services,
Security and Identifier Registration**

Second Edition — 2016

International Civil Aviation Organization

AVA **Documents**
Document Sharing Hub

Published in English only by the
INTERNATIONAL CIVIL AVIATION ORGANIZATION
999Robert-Bourassa Boulevard, 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 Identifier Registration**

Order Number: 9880P4

ISBN 978-92-9258-143-5

© ICAO 2017

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, without prior permission in writing from the International Civil Aviation Organization.

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

[illegible][illegible]

(iii)



Documents

Document Sharing Hub

TABLE OF CONTENTS

	<i>Page</i>
Foreword	(vii)
Acronyms	(ix)
Chapter 1. Introduction	1-1
1.1 Overview	1-1
1.2 References.....	1-1
Chapter 2. Directory Services.....	2-1
2.1 Introduction	2-1
2.2 System Level Provisions	2-4
2.3 Directory Object Class and Attributes Specification	2-6
2.4 ATN Directory System Schema	2-16
2.5 ATN Directory Protocols.....	2-39
Chapter 3. Security	3-1
Chapter 4. Identifier Registration	4-1
4.1 Introduction	4-1
4.2 ATN identifiers	4-1

Document ID: 123456789

FOREWORD¹

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 and Identifier Registration (replaces Doc 9705, Sub-volumes I, 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
- Chapter 2 DIRECTORY SERVICES, provides the detailed technical specifications for the ATN directory services
- Chapter 3 SECURITY SERVICES, provides the detailed technical specifications for the ATN security

¹ The first edition of this manual amended and replaced the third edition of the *Manual of Technical Provisions for the Aeronautical Telecommunication Network (ATN)* (Doc 9705).

services

Chapter 4 IDENTIFIER REGISTRATION, provides the registration of ATN identifiers and associated provisions

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

(x)

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 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 programme 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.

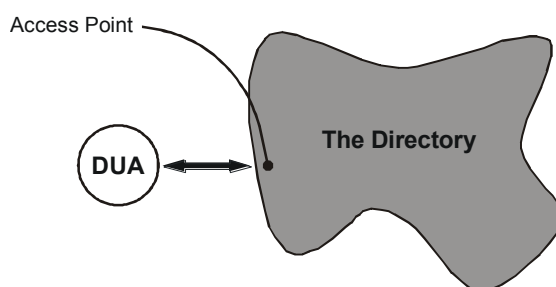


Figure 2-1. Access to the ATN DIR

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 2-2.

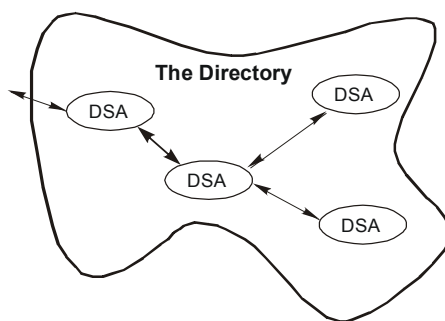


Figure 2-2. Functional model of the ATN DIR

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

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

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 2.5.

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

2.3 DIRECTORY OBJECT CLASS AND ATTRIBUTES SPECIFICATION

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

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

<i>Ref. no.</i>	<i>Object class</i>	<i>Base</i>	<i>Basic profile</i>	<i>DL profile FG</i>	<i>ATN DSA</i>
1	mhs-distribution-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 2-2.

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

<i>Ref.</i>	<i>Object classes</i>	<i>ATN DSA</i>
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
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

2.3.2.4.2 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

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.

2.3.3.1.2 Table 2-3 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. 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	
C1 = If p_strong_rep then M else O.					

2.3.3.2 DSA collective attribute types defined in ISP 15126-1

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

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 2-4.

2.3.3.3.2 Table 2-4 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. 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
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 2-5.