International Civil Aviation Organization

Fifth Meeting of Aeronautical Telecommunication Network (ATN)
Transition Task Force

Phuket, Thailand, 9-13 June 2003

Agenda Item 4: Review the development status of ATN technical documents

Status on Development of Document on the Use of Directory Services

(Presented by the Rapporteur of the ATNTTF Ad Hoc Working Group)

Summary
This paper presents the status on the work to define the use of the ATN Directory Services within the Asia/Pacific Region.

1 Introduction

As part of its work program, the Ad Hoc Working Group B has undertaken the development of planning documents for the use of the ATN Directory Services within the Asia/Pacific Region. It was expected that the work would result in completed documents in time for this meeting of the ATNTTF. However, the work has progressed more slowly than expected and is not entirely complete at this point.

2 Overview of the Work

The Working Group has progressed a document through 3 drafts that presents an overview of the ATN Directory Services and establishes which of the object classes (data base record types) and attributes (contents of each record type) will be supported in the Region. The current draft of the document has complete lists of object classes and attributes that are now out for comment and consensus.

3 Further Work

The current document needs further review of the information currently provided. This should be achieved at the next Ad Hoc Working Group B meeting. After agreement on the object classes and attributes, additional sections providing profiles of the access and exchange protocols for the ATN Directory need to be provided. This work will begin at the next Ad Hoc Working Group B meeting and should be completed within one year.

4 Recommendations

The ATNTTF members are asked to take under consideration the status of the current work and to authorize the Ad Hoc Working Group B to continue progressing this effort.

International Civil Aviation Organization

Fifth Meeting of Aeronautical Telecommunication Network (ATN)
Transition Task Force of APANPIRG

Phuket, Thailand, 9 – 13 June 2003

Agenda Item 4: Review progress on the technical documents

Third Draft Asia/Pacific Technical Document on Use of Directory Services

(Presented by the Rapporteur of the ATNTTF Ad Hoc Working Group)

Summary

This paper presents a third draft of information relating to the application of the ATN Directory Services to Asia-Pacific Region.

1 Introduction

The introduction of the ATN applications, especially AMHS, changes the way that information is exchanged within Administrations as well as between States. The ATNP recognized that the need for the exchange of information could best be provided through the definition of a directory service. The definition of the directory services was completed and published as Sub-Volume 7 of Doc. 9705 edition 3.

This document presents information on the planning of implementation of the ATN Directory Services (ATN-DS) within the Asia/Pacific Region.

1.1 Definitions and Acronyms

ATN
AMHS
ATN-DS

BIS
ICAO
DSA
DUA
DMD
DIT

2 Asia-Pacific Background

The Asia/Pacific Region is moving rapidly towards deployment of both an ATN infrastructure (backbone routers) and the ATN AMHS. In conjunction with these implementations it would be advantageous to begin implementing the ATN-DS to ease the transition to the use of AMHS and for the future use of both air-ground applications and the implementation of security.

3 Overview of Plan for ATN Use

1.1. Description of AMHS Plans
1.2. Description of Air-Ground Application Plans

4 Overview of ATN Directory Services

The ATN-DS is defined in Sub-Volume 7 of the third edition of ICAO Doc. 9705. It defines the ATN-specific directory schema and the protocol subsets needed to store, retrieve, and use the associated entries. The following sections present an overview of the current ATN-DS definition.

4.1 Rationale for ATN-DS

The ATN employs increasingly sophisticated applications that must work on and across computer networks and systems from multiple States and vendors. An X.500-based Directory Service constitutes one of these distributed applications and at the same time can provide significant support to the realization of other distributed applications.

4.2 X.500 Directory Information Concepts

4.2.1 X.500 Data Model

The information repository of the ATN Directory is a distributed database, capable of storing information about people and objects in various nodes or servers distributed across a network. It is these servers, acting in concert, which provide the potentially global access to information made possible by X.500 technology.

Distributing information in this manner has various advantages over the conventional method of centralizing information storage, for example:

- The information is kept "close" to those people or processes which are most likely to make heaviest use of it or to be responsible for keeping it up to dates – this is likely to reduce access time and network costs, and increase the likelihood of the accuracy of the stored information;

- Since the information is distributed across several servers, the impact of a given server becoming inactive, for whatever reason, is only to make unavailable the information for which that server is responsible, rather than bringing down the entire database, as would be the case if a centralized server were to go down;

- The ATN Directory has the capacity to grow indefinitely in size and storage capacity through the simple addition of new nodes. Such growth might be achievable but would be less practical with a centralized system.

The ATN-DS database is distributed across directory servers called Directory Service Agents or DSAs. The ATN-DS data that is maintained by the DSAs is defined using a structure known as the Directory Schema. The information held by the ATN-DS is collectively termed the Directory Information Base (DIB), and the organization of the data within the DIB is defined by the Directory Information Tree or DIT.

The DIB is made up of entries, each one of which describes a single object in the real world (for example, "person"). Objects are defined by an ***object class*** definition. The contents of an entry (object class) is a group of features used to describe that object called ***attributes***. Each attribute in turn has a type and one or more values (for example, the entry for the object "person" may have a "telephone-number" attribute with one or more telephone number values). In addition, there may be one or more context values per attribute value. These context values are used to specify information that determines the applicability of that attribute (for example, a context would be used to tell how a time or date value should be interpreted). Figure 4.2-1 depicts these relationships.

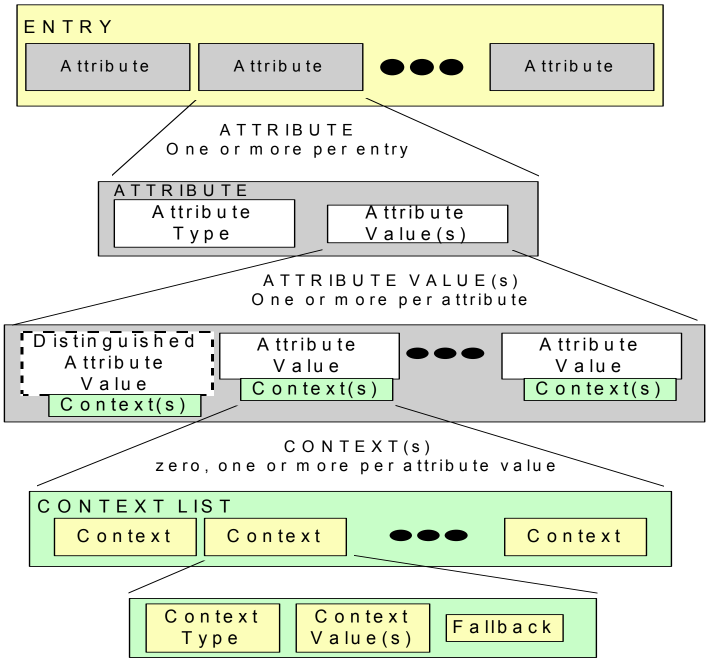


Figure 4.2-1 Directory Entry Structure

The DIT defines the organization of the information of the DIB by defining logical hierarchies of objects classes.

The structure defined by the DIT provides the mechanism for the naming of objects in the DIB. Each entry in the ATN-DS has a Relative Distinguished Name (RDN) that identifies an entry (in Figure 4.2-2, {country = “US”}, {organization = “XYZ, Inc”} and {locality = “Boston”} are all examples of RDNs). The sequence of RDNs all the way to a leaf, or end, node is a distinguished name (DN). The DN is a globally unique identifier for a directory object. In Figure 1, the DN for the research department of XYZ, Inc is {country = “US”, locality = “Boston”, organization = “XYZ, Inc”, organizational unit = “Research”}. Note that the alias entry for {organizational unit = “Production”} is under the Canadian company, so there are two valid, but unique, DNs.

The Directory specifies a set of rules called the Directory schema that dictates the types and attributes valid for DIB entries. In addition, a Directory system schema dictates how operational information (e.g. create/modify time stamps, administrative roles, etc) is stored in the Directory.

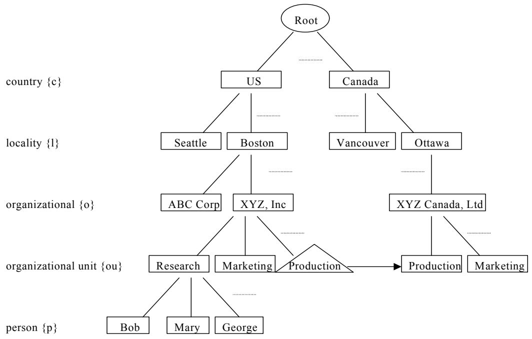


Figure 4.2-2 Directory Schema

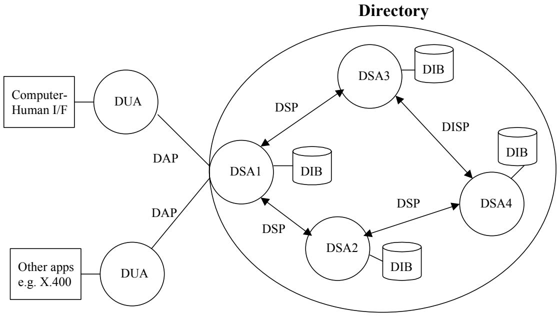
Note: The directory schema shown in Figure 4.2-2 only shows a partial schema based upon the country-based schema. An additional branch of the schema (not shown) is organization-based and has the organization attached directly to the root node.

4.2.2 X.500 Directory Protocol Concepts

The ATN-DS user (person or process) accesses the ATN-DS via a client process, known as a Directory User Agent (DUA). The DUA interfaces with the ATN-DS using a protocol between itself and one of the ATN-DS servers, termed Directory System Agents (DSA). Usually the DSA contacted would be the one closest, in terms of connection cost or organizational affiliation, to the DUA.

The DSAs and the information that they store in their respective DIBs comprise the ATN-DS. The DSAs also communicate between themselves via a set of protocols, which embody a set of operations that may be performed on the ATN-DS information. Each DSA knows how to contact a number of other DSAs (at least one). This is the mechanism through which a request for information can be propagated throughout the distributed directory: if a particular DSA is unable to satisfy a request, the request is forwarded to another DSA which is more likely to have the necessary information, and so on.

There are four kinds of protocols associated with the ATN-DS: the Directory Access Protocol (DAP), Directory Systems Protocol (DSP), Directory Information Shadowing Protocol (DISP) and the Directory Operational Binding Protocol (DOP). These protocols provide the means for the various ATN-DS agents—the Directory User Agent (DUA) and Directory Service Agent (DSA) to perform operations on the DIB. Figures 4.2-3 and 4.2-4 show two different views of the ATN-DS model, and are further explained below.



Note: DOP is not shown, but could take place between DSA pairs
DSA1-DSA2, DSA1-DSA3, DSA2-DSA4

Figure 4.2-3 Directory Model

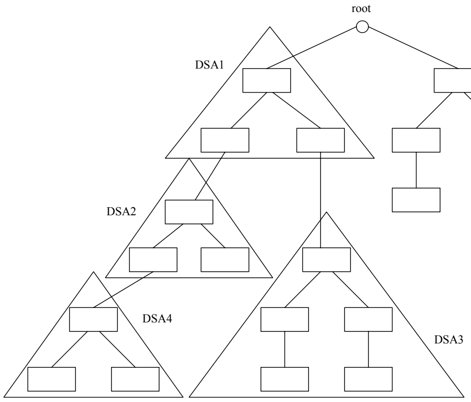


Figure 4.2-4 Directory Model Showing DSAs

Users access the ATN-DS via the DUA. Note that the user can either be a human or an application. The DAP provides the means for the DUA to communication with the DSA. The DSA manages the information in the ATN-DS. DSAs communicate with each other via the DSP (for distributed directory operations, e.g. search and read as directed by a DUA command) and DISP (for DIB replication transfers). The DOP defines the operational relationship (i.e. administrative agreements) between pairs of cooperating DSAs. Note that the DAP and DSP also make use of the Remote Operations Service Element (ROSE) and Association Control Service Element (ACSE) ASEs. Note that some actions, like the DSA interface to the local DIB, is beyond the scope of the ATN-DS.

The DUA has a number of operations it can perform with the DSA. These include read (read, compare, abandon), search (list, search) and modify (add entry, remove entry, modify entry, modify RDN) operations. The DSA, upon receipt of a query from the DUA, can perform basically the same operations, but are predicated with "chain" which implies that the DSA will pass on the request to as many DSAs as necessary in order to complete the request. There is also a "referral" response, which a DSA can return to either the requesting DSA or DUA. The referral response is used when the DSA has knowledge of the proper DSA to contact (i.e. name and address). The DSA or DUA that receives the referral response can then contact that DSA directly in order to carry out the operation.

The DOP has two types of bindings that can be established: the Hierarchical Operational Binding (HOB) and Shadow Operational Binding (SOB). The HOB governs the relationship between a pair of DSAs, such as DSA1 and DSA2 in Figure 4.2-4. Some properties of the DIT governed by DSA1 will apply to the DIT governed by DSA2. The HOB provides a mechanism for the subordinate DSA (e.g. DSA2) to receive any administrative information from its superior DSA (e.g. DSA1). The SOB is responsible for setting up the binding necessary between two DSAs so that replication can take place. This typically involves determining the portion of the DIT to be copied as well as the supplier and consumer DSAs. Once this binding is known, then the DISP can be used. The DISP consists of three operations, Coordinate Shadow Update, Request Shadow Update, and Update Shadow. These operations all involve the replication of DIT information.

4.2.3 Detailed X.500 Data Concepts

4.2.3.1 Directory Schema

The ATN Directory Schema constitutes the framework within which ATN-DS information is stored. It consists of a set of rules and definitions, which define the naming of entries, the content of attributes and entries, the structure of the ATN-DS as whole and hierarchical relationships between entries.

The Schema comprises the following components:

- **Name Form** definitions, which describe how ATN-DS entries should be named;
- **DIT Structure Rules**, which define hierarchical relationships between entries of different object classes;
- **DIT Content Rules** definitions, which allow the inclusion in entries of attributes not indicated in the entries' structural object classes;
- **Object Class** definitions, which are used principally to distinguish between entries representing different types of object.
- **Attribute Type** definitions, which holds information regarding a particular quality or characteristic of an object represented by a Directory entry.
- **Matching Rule** definitions. Each attribute has associated with it a set of matching rules, which determine how values of the attribute may be matched against other values.

4.2.3.2 NAME FORM

Each entry in the ATN-DS is identified by at least one unique name, called the entry's Distinguished Name (DN). The DN is formed in the following fashion:

- The DIB is organized into a tree-shaped hierarchy, the Directory Information Tree (DIT), in which each entry has exactly one superior entry but may have many subordinate entries. This organization is illustrated in Figure 4.2-5.

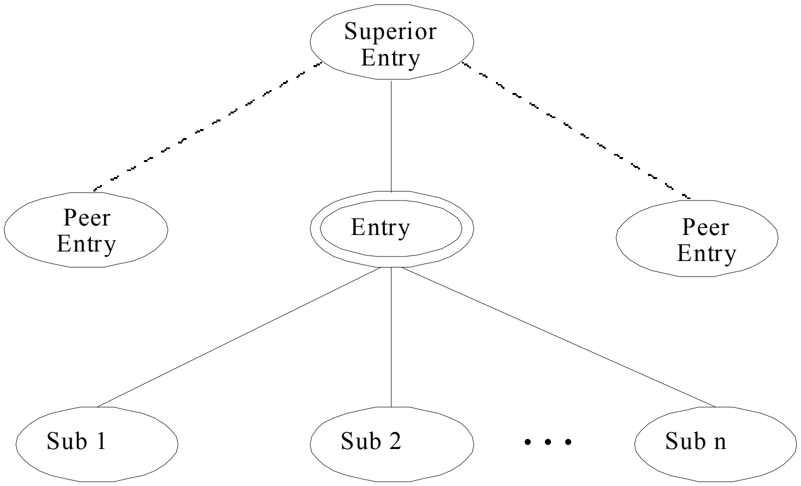


Figure 4.2-5: **The basic structure of the Directory Information Tree.**

Clearly, each superior entry may have many subordinates, so the entry may be one of many siblings at the same level in the tree:

– Each entry contains at least one attribute value, which is designated as the entry's name at that level, i.e. relative to all its siblings. This name, known as the entry's Relative Distinguished Name or RDN, must be unique among all the entry's siblings.

– The unique name of the entry, it's Distinguished Name or DN, is formed by the concatenation of the RDN of the entry with those of each of its superiors, from the top of the DIT on down to the entry.

4.2.3.3 DIT Structure Rules

The placement of entries within a portion of the DIT is governed by rules set out by the responsible authority, known as *DIT Structure Rules*. Each entry in the Directory contains an attribute of type **governingStructureRule**, which holds the structure rule that governs the possible placement of the entry. The entry may only be placed in a portion of the DIT if the Directory schema holds a DIT structure rule that matches that held in the entry.

The DIT structure rule consists of 3 parts:

1. A unique identifier;

2. A name form identifier, which specifies the name form that entries governed by this structure rule will take;

3. A list of superior structure rule identifiers, which denote where in the DIT the entry may be placed, i.e. which classes of entry it may be placed subordinate to.

4.2.3.4 DIT Content Rules

The content of an entry, in terms of the attributes it contains, is regulated primarily by the entry's structural and auxiliary object classes. However, additional contents may be specified by the definition of a *DIT Content Rule* associated with the entry's structural object class.

A DIT content rule specifies the following:

- The identifier of the structural object class to which it applies;

- The identifiers of the auxiliary object classes permitted in entries governed by the rule (optional);

- The identifiers of the mandatory attributes required for entries governed by the content rule, in addition to those mandated in the structural and auxiliary object classes (optional);

- The identifiers of the optional attributes required for entries governed by the content rule, in addition to those named in the structural and auxiliary object classes (optional);

- A list of identifiers of optional attributes from the entry's structural and auxiliary object classes that the content rule precludes from appearing in entries governed by the rule (optional).

Note that, unlike the characteristics of an object class, those of a DIT content rule are *not* inherited by any subclasses of the object class to which it applies.

DIT content rules are thus useful in the following ways:

- They permit the modification of an object class at a particular level in the object class hierarchy, while avoiding the inclusion of the modifications into the object class chain;
- They permit the exclusion of certain optional attributes from entries of a given object class without modifying the object class itself;
- They allow the inclusion of individual attributes into entries, without reference to other object classes.

4.2.3.5 Object Classes

ATN-DS object classes are used principally to distinguish between entries representing different types of object. Each ATN-DS entry must belong to at least one object class, and contains an attribute, the value(s) of which indicate(s) the object class(es) to which the entry belongs. Following from this descriptive function, the entry's object class serves several specific functions within the Directory:

- It governs the attributes the entry contains;
- It governs the *position* the entry may take in the Directory structure;
- It governs the *administrative policy* associated with the entry.

Object classes may be defined in international standards, by other standards or implementer bodies, by vendors, or by users (private object classes). The mechanism for object class definition is described in Section 12.3.3 of [ISO 9594/2]. The ATN-DS contains a set of ATN-specific object classes for use within the context of the ATN.

5 Overview of ATN Directory Services Concept Of Operations

To support the addition of directory services to the ATN, it was necessary to develop a directory services concept of operations. The concept of operations was published in the second edition of the ATN guidance material (ICAO Doc. 9739). Much of the following description is based upon that text.

5.1 Architecture Model

5.1.1 Domains

The ATN-DS is based on the ITU-T X.500 directory model. That model includes the concept of Directory Management Domains (DMDs). A DMD consists of the DSAs and DUAs managed by one organization, plus the DIT entries that are mastered on those DSAs. A Directory Service constitutes the directory information and operations (services) provided by one or more DMDs to a community of users. The ATN Directory Service, which serves the entire set of CAAs and Organizations, includes or involves several DMDs as depicted in the following figure.

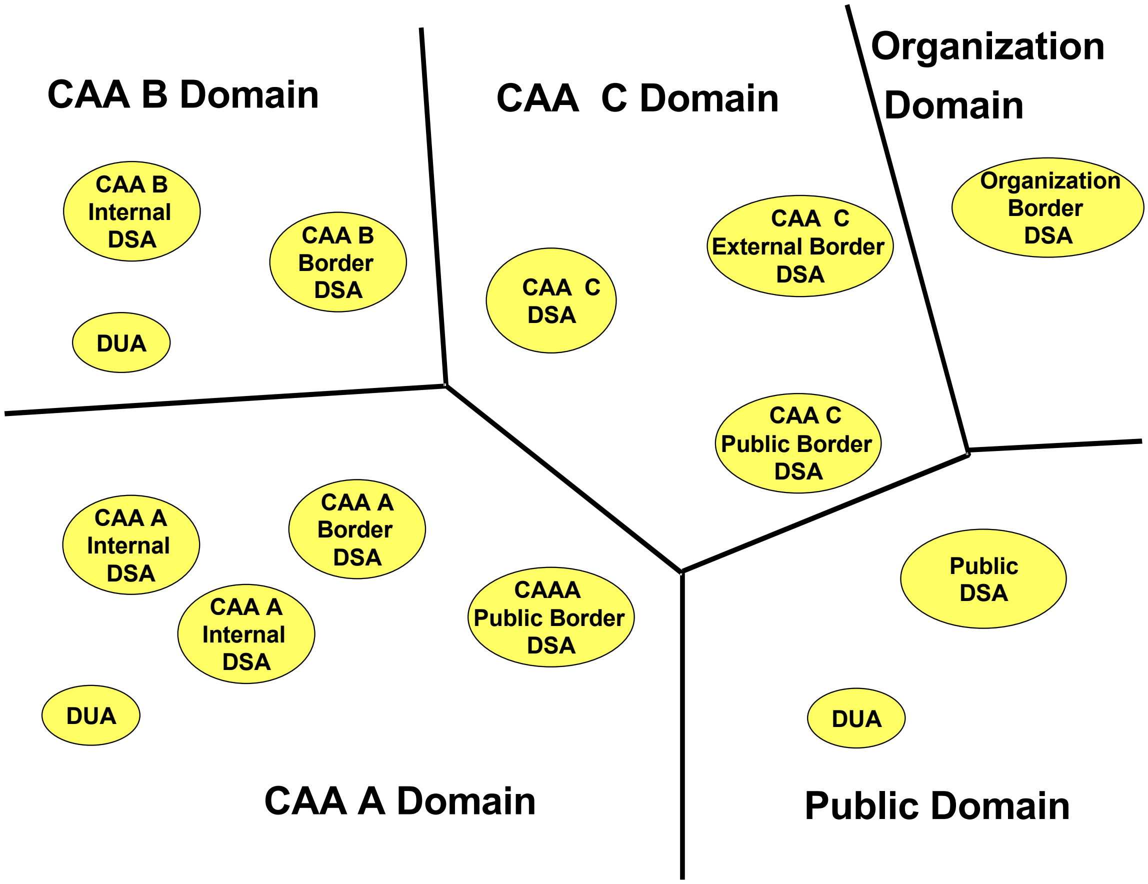


Figure 5.1-1: DMDs in the ATN Directory Service Architectural Model

Each CAA or Organization constitutes its own DMD. The ATN-DS consists of those DMDs that are the top nodes in the ATN DIT (either c=<country, o=<caa> or o=<organization>). Each DMD is managed by the owner of the DMD. There is no central agency managing the ATN Directory Services. The public domain constitutes general Directory Services provided to the public outside of CAAs and Organizations ascribing to the procedures of ICAO and the ATN and is actually a conglomeration of public Directory services and cooperating DMDs.

Directory domains are linked to provide an integrated Directory Service. Of interest are the following Directory Services:

a. CAA and Organization Directory Services provided to the staff (e.g., over intranets);

b. the overall ATN Directory Service provided across the ATN;

c. specific external Directory Services the CAAs and Organizations may participate in for a community of users not necessarily open to the public; and

d. the Public Directory Service provided to the public at large.

DMDs are linked to provide these services through the use of Border DSAs. Border DSAs are those owned by or operated on behalf of one domain but participate in the Diretory Service of a broader domain and are accessible from users and/or DSAs in that broader domain. Border DSAs act as the interface and interconnection points (inwards to internal information, outwards to external information). The terms "Public Border DSA" and "External Border DSA" are used to distinguish such DSAs that are participating in a Public Directory Service or Extranet-based Directory Service respectively.

The figure 5.1-2 illustrates how the Directory Services map to the physical components and DMDs.

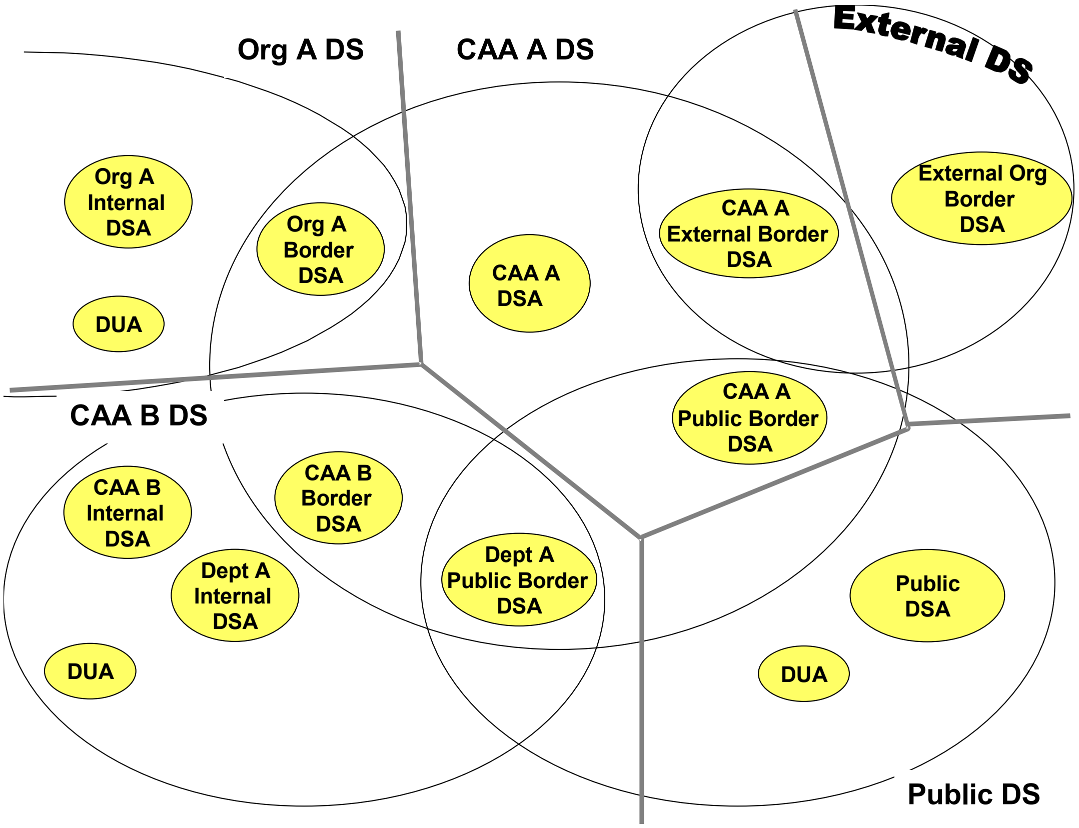


Figure 5.1-2: Directory Services

Through the public domain the ATN Directory Services may be connected into the global Directory Service.

The Border DSAs, owned and operated by CAAs and Organizations, are participating in the ATN-DS and are in a different integrity sub-domain/network than the internal DSAs. Similarly, Public Border DSAs are participating in the Public Directory Service and are thus in a low integrity sub-domain.

The Border DSAs provide the logical linkage between domains and allow a larger Directory Service to be built from what would otherwise be islands of directories. Two types of linkages are possible: chaining, in which requests are passed along from one domain to another, and shadowing, in which information is copied between domains so that requests can be answered within a domain other than the domain owning the master entry. The ATN Directory Architecture may use both kinds of linkage. Chaining is predominantly carried out using the DSP protocol and shadowing is predominantly carries out with the DISP protocol; this is how the different linkages are shown in the diagrams in this specification.

Note: There is a third way of retrieving information from remote DSAs, known as referral. This method does not require the linkage between DSAs but requires that a DSA have knowledge about what information is contained in other DSAs.

The figure 5.2-3 illustrates the minimum connections Border DSAs provide.

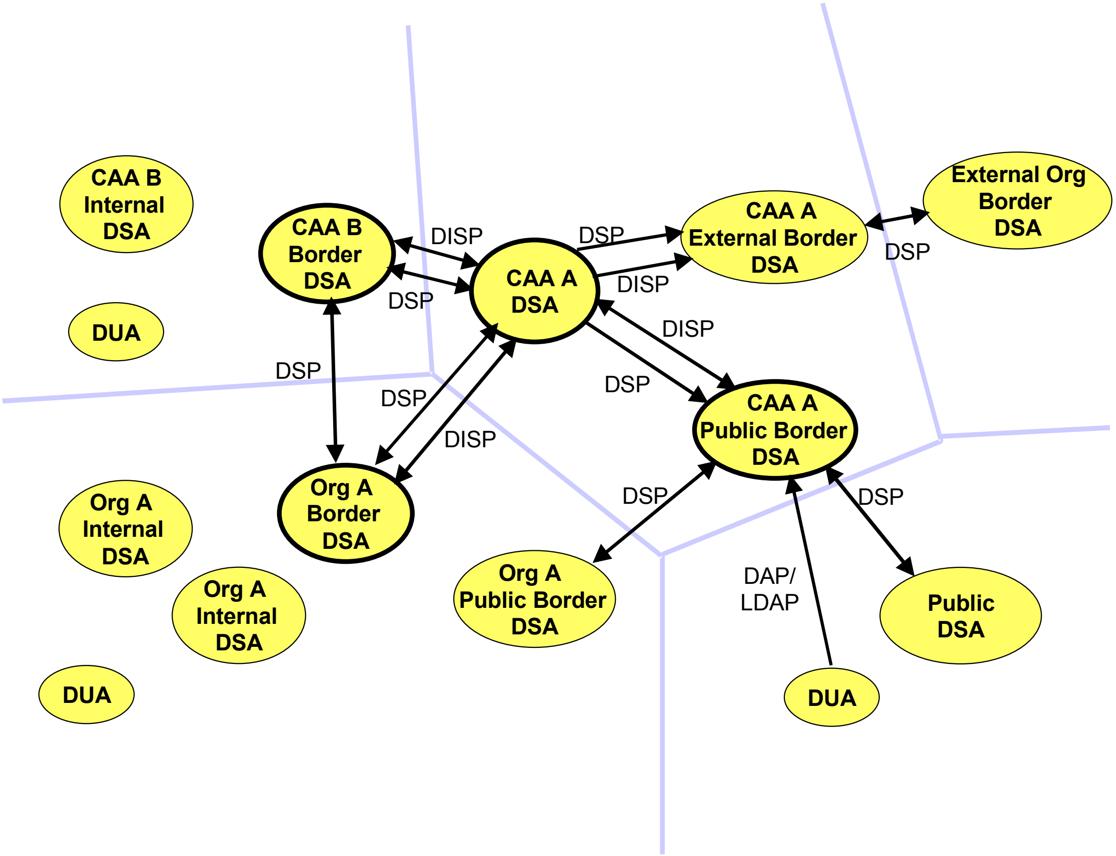


Figure 5.2-3: Minimum Connections

The following sections examine the CAA domains in detail, describing the mandatory and recommended connections, and the information that flows across them.

5.1.2 CAA and Organization Domains

Each CAA or Organization is responsible for its own DMD. The management of the DSAs and DUAs within a DMD's domain is the responsibility of the owner of the DMD but the management may be delegated to another organization or State. The owner of a DMD is responsible for the definition and management of its own DIT sub-tree which is mastered on its own DSAs.

Each CAA may field a Border DSA which is the DSA designated as the interface point to the CAA's Directory Service for the ATN-DS. A CAA may also have one or more Internal DSAs, but the Border DSA is the CAA's connection into the ATN-DS. A CAA will typically choose to have a distinct DSA for this purpose, separated from its internal network with appropriate security/access controls. The internal network of DSAs can be considered a high integrity domain since it is under the control of one DMD, services a small community of users and can be protected on an intranet. The Border DSA and ATN domain are considered a medium integrity domain since they require cooperation between several DMDs, service a large community of users and are protected on the ATN.

If a CAA chooses not to implement X.500 protocols internally, it will still need to field an X.500 compliant Border DSA in order to participate in the ATN-DS. The CAA must ensure that any internal Directory Service is capable of making requests (for external information) to the Border DSA. The CAA must also ensure that the Border DSA is capable of presenting the appropriate information to the ATN-DS.

The figure 5.2-4 shows an example of the minimum information a department in a CAA masters and shadows at the domain boundary.

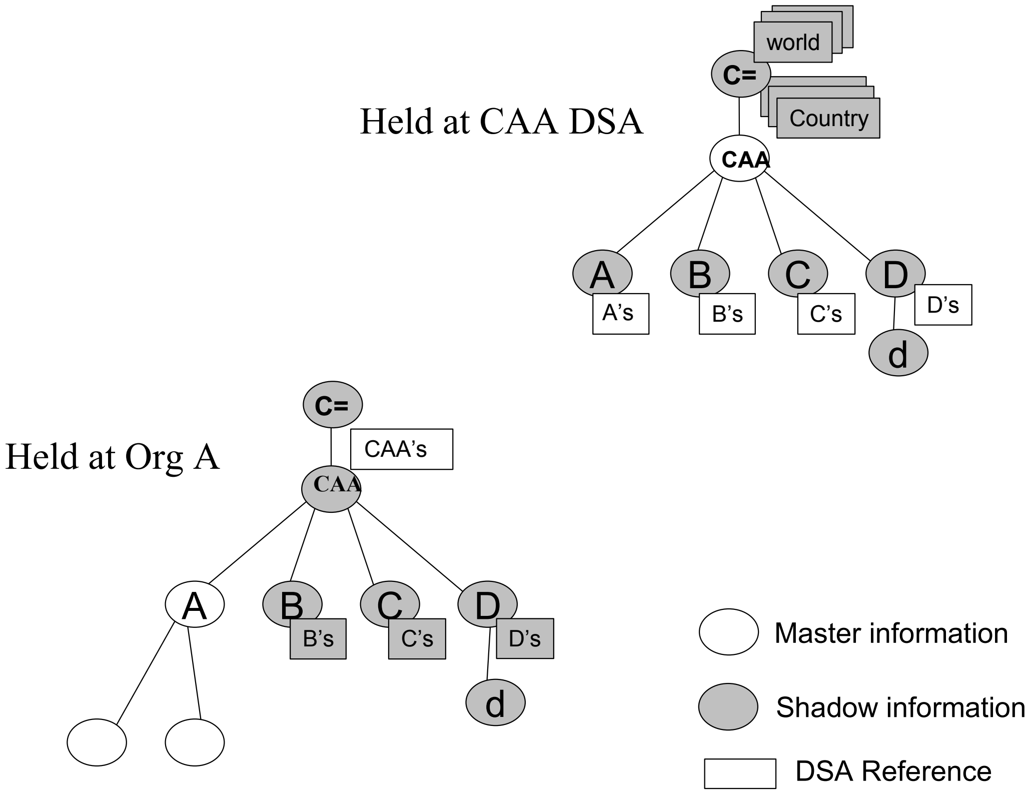


Figure 5.2-4: Minimum Information Mastered and Shadowed

A CAA may hold shadows (copies) of the c=<country> and o=<caa> entries and may maintain a superior reference (pointer) to that CAA's DSA. It may hold shadows of other organizational (ou) entries (e.g., B, C, D) in its domain and may maintain references to the Border DSAs of other CAAs, all of which it will obtain through shadowing between its Border DSA and other ATN DSAs. It may also hold information from other departments (e.g., d) which is considered to have a high availability requirement. This will also be shadowed across other ATN DSAs.

The connectivity requirements are shown in the following figure. Minimal requirements are shown with bold/thick lines. Recommended or optional connectivity is shown in normal lines.

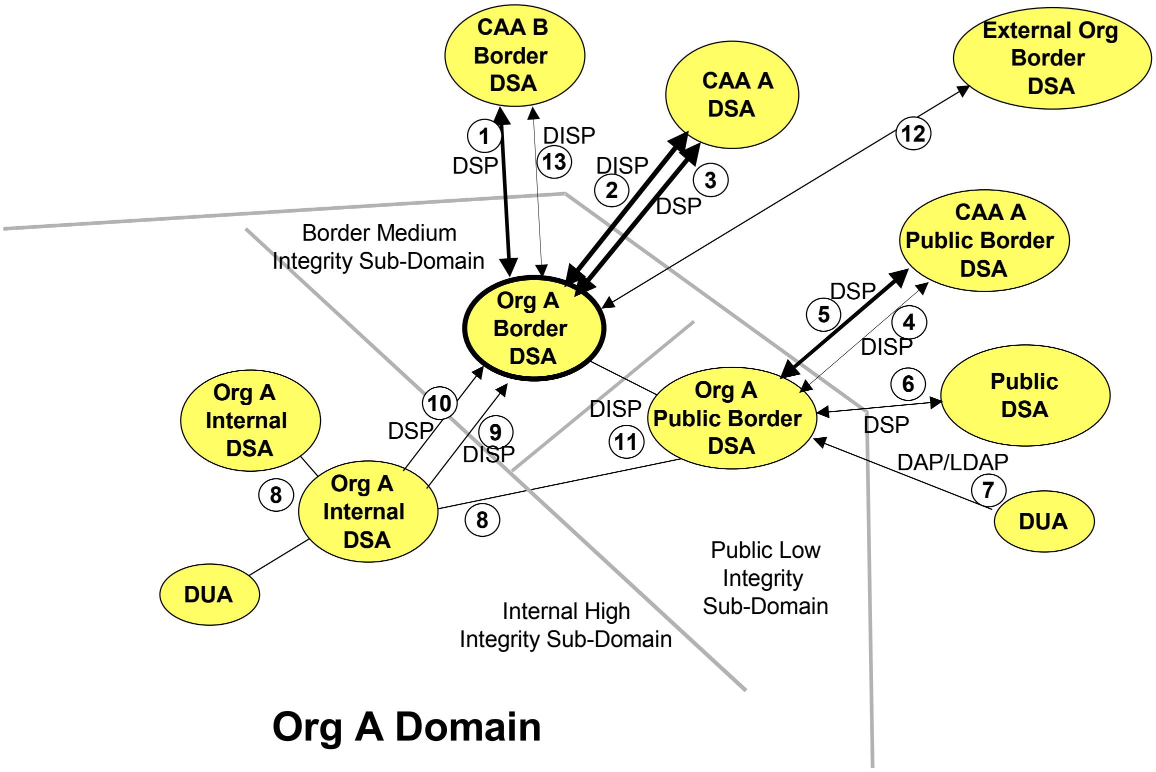


Figure 5.2-5: Connectivity Requirements

The Border DSA may support DISP shadowing with the other CAA DSA (2) in order to supply its own o = <caa> entry plus high availability information from its own subtree, and to obtain the shadowed external information and knowledge references described above. CAA policy may determine if external directory information will be further copied from the Border DSA to the Internal DSAs in the CAA.

The Border DSA may accept DSP chaining of requests from other Border DSAs (1) (3). A CAA may decide whether such requests are ever chained into internal DSAs or whether it is always answered from information it holds itself. It is recommended that a Border DSA always answer external requests instead of chaining inwards. This requires it to hold all information a department wishes to make available to an external domain. This information is mastered on the internal DSAs and periodically shadowed (9) to the Border DSA using DISP or other means (such as bulk file transfer).

The Border DSA chains outwards (1,3) any internal requests (10) for external information it does not have. The Border DSA is able to chain requests directly to another CAA's Border DSA (1) for information that is located in another CAA's DIT subtree.

Information which a CAA wishes to make available in the public domain may be shadowed to other DSAs for further distribution (2). Alternatively, a CAA may choose to field its own Public Border DSA and to shadow the information to it using DISP or other means (11). The Public Border DSA may accept chaining (6) from DSAs in the public domain in general, and even direct DAP/LDAP requests (7) over the internet. It may accept chaining from other government Public Border DSAs (5) and maintain, through shadowing (4) of entries and knowledge references.

The inner structure and behavior of CAA Directory domains are up to the CAAs (8 - 11). CAAs may also have communication links to external organizations (12) and direct shadowing with other CAAs (13) beyond that described here.

The Border DSA function needs to be highly available and reliable. Each State and Organization needs to design its Border DSA(s) to achieve the required availability (e.g., 99.5%) of the Directory Service (information access) 24 hours a day, 7 days a week. Reliability of the service may be achieved by several means at the CAA's discretion.

There needs to be a high level of assurance that only the allowed components interact for the purposes for which the architecture model indicates. Ideally, the DSAs in a CAA Domain may be capable of strong authentication between themselves and with other DSAs. However, the assurance may be achieved through network level security features.

6 Usage of ATN Directory Services

6.1 Use of ATN-DS by AMHS

The ATN AMHS is defined in a way that the use of directory is not mandatory until edition 3. Even at that point, use of the ATN-DS is optional. The ATN-DS is particularly suited to the AMHS application since significant information about users and other AMHS systems may be obtained directly from the ATN-DS.

6.1.1 Retrieval of Addressing Data

The ATN AMHS requires the mapping of user names (email addresses) to a series of specific AMHS attributes including the MTA name of the next system and the NSAP of the next hop routing.

If an implementation does not support the ATN-DS, this information must be maintained locally in tables. As in the case of any table driven approach, the administration of the tables may require significant resources.

The use of the ATN-DS greatly simplifies the retrieval of addressing information. The MTA can map to the complete set of addresses for MTA routing based on a query to the

DSA. The query response will return the information that will be used within the lower layer protocol connection establishment.

The ATN-DS will also be useful in the conversion between AFTN and AMHS addresses since the information will be in the appropriate user records. This will make transition seamless since the presence or absence of certain address types will indicate the type of user.

6.1.2 Retrieval of MTA Capabilities

As AMHS is deployed, MTAs with different capabilities will be implemented. The selection of which options to use and the capabilities of a remote MTA will become a problem or MTAs will be required to use the minimum mandatory features. This is a place where the ATN-DS can provide significant assistance. Within the DIB, descriptions of MTA capabilities will be available through standard directory queries.

6.2 Use of Directory Services by Context Management

As the concept for the ATN evolves and implementations are started, modifications in order to support security measures and directory interaction become necessary. Some of the guidelines that have to be kept in mind while meeting the security requirements set out by the ICAO Panel are:

- Performance impacts, including message sizes, numbers of transactions, impact on transaction times, etc should be minimized

- Interoperability considerations of the new features with previous versions of applications

- Operational concept impacts, e.g. an application should not have to behave significantly different with the new enhancements, nor should new features preclude a previously defined operational need

- SARPs impacts and changes

After careful consideration and much debate, it was decided that security could be best implemented through changes as presented in Edition 3 of Doc 9705. The security enhancements make use of CM for key information and key usage exchange for all air-ground applications. Additionally, all of the air-ground applications are modified slightly in order to provide the Dialogue Service (DS) with new security parameters.

Security introduces new functionality to the air-ground applications. The main impacts of security as far as applications are concerned are exchanging keys, giving an indication of the domain those keys are valid for, indicating to the DS the level of security that is required, and ensuring that received primitives are consistent with the local security policy. Since all applications must be able to pass the new DS parameters and check to make sure they are consistent with local security policy (in itself no too big a change), the remaining decision is how to pass the key and key usage information—whether it should be done on a per application basis or by CM on behalf of the other applications.

6.2.1 The CM Security Concept

CM was chosen as the means to exchange key and key usage information between aircraft and ground systems. The modifications to the CM application itself consist of additional D-START parameters for air- and ground-initiated services and user data on ground-initiated services. These modifications also retain backwards compatibility with version 1 CM applications. As previously mentioned, if each air-ground application had to perform its own key exchanges, there would have to be new services to negotiate this, along with corresponding new user data to support the key exchange. There might also be more duplication of key negotiations, as there may be no indication of domain usage per application (i.e. a CPDLC application in one facility might not know if a CPDLC application in another can use the same key, so there could be multiple key negotiations when in fact they are not needed). The CM security and directory modifications alleviate these problems, and in fact provide solutions to others (e.g. how to get downstream facility application information, including security information).

The way CM operates with security is very much the same as it operates without security. A CM-air-user indicates whether or not a secure logon is required (based on local requirements; however the ground has the ultimate decision on whether or not security is required for its airspace). If security is required by the ground system and correctly requested by the aircraft, then the ground will return application information, including security information, for each application the aircraft supports. Note that the ground should not send key information for an application that was not indicated in the CM-logon request by the aircraft. This is easily controlled by local policy. The security information provided for each application includes the public key and a domain usage indicator. The domain usage indicator is a Boolean; if set to true then the key that is provided for that application will work for all other applications within that CM domain (signified by the ADM field of the NSAP). If not provided, new key information must be obtained for another facility within that CM domain. This determination will be based upon the local security architecture.

Additionally, secure versions of the CM-forward and CM-update have been added, which allow the use of the CM-forward/CM-update combination for secured services. For the secure CM-update, not only has key information been added to the user data (as for a secure CM-logon response), but a facility designation field has been added as well. This allows, for example, a CM facility which has just completed a secure CM-logon service with an aircraft to send to that aircraft a secure CM-update identifying the facility designation, CPDLC application information, and key information of the facility with which the aircraft needs to perform an NDA connection. This can be done during a non-time critical period (such as before pushback). Then the ground system can perform a CM-forward (or some other local ground-ground forwarding service) to give the aircraft information to that NDA facility. Now both the NDA ground system and the aircraft have all of the necessary information for secure services with each other, which will save time when the actual connection needs to be made. If need be more secure CM-updates may be invoked in order to give the aircraft additional information such as en route FIS facilities' addresses and security information.

6.2.2 CM Directory Concept

The last section described at a high level how security works between peer applications (air-ground and ground-ground). However, an important step was not described: how is the key information for the applications retrieved by the ground CM application? The answer is via a directory service. The CM SARPs recommend that the ATN Directory service as specified in Sub-volume 7 be used. The ATN Directory service is an X.500-based directory that contains all of the information and basic protocols necessary for ATN operation. It can also function in a secure mode, which will allow cross-domain key information requests. It should be noted that there will still need to be additional requirements developed in order to perform Directory services, and that implementing states will need to perform more in-depth operational analysis and develop operational concepts for the implementation of Sub-volume 7 services. However, the tools necessary are already in Sub-volume 7, and the user requirements are in the CM SARPs. Additionally, AOC applications can make use of the same directory in order to obtain application and security information.

While one of the main functions of the directory concept is to enable secure ATN services, additional capability afforded by a directory becomes evident. This is the ability of a CM application to obtain, in a standardized way, information for other facilities as well as provide to the directory information about itself and aircraft it has performed services with.

7 Application of ATN Directory Services to Asia-Pacific Region

7.1 Use in support of General ATN Operation

The Asia/Pacific Region is moving towards the implementation of a complete ATN infrastructure. Within this environment,

7.2 Use in support of AMHS

The States within the Asia/Pacific Region is expected to begin to deploy the ATN-DS as soon as significant experience is gained in the deployment of the AMHS.

7.3 Use in support of Air-Ground Applications

The use of the ATN-DS in support of air-ground applications is expected. The main purpose of using the ATN-DS is to provide an infrastructure for implementing security services.

8 Directory Services Data Definitions

Table 8-1 ISO/IEC 9594-7:1995 Object Classes as Specified in ISO/IEC ISP 15126-1

Ref. No.	Object Class	ATN DSA	Use in Asia/Pacific
1	top	m	Y
2	alias	m	Y
3	country	m	Y
4	locality	m	Y
5	organization	m	Y
6	organizationalUnit	m	Y
7	person	m	Y
8	organizationalPerson	m	Y
9	organizationalRole	m	Y
10	groupOfNames	o	N
11	groupOfUniqueNames	o	N
12	residentialPerson	o	N
13	applicationProcess	m	Y
14	applicationEntity	m	Y
15	dSa	m	Y
16	device	m	Y
17	strongAuthenticationUser	m	Y
18	certificationAuthority	m	Y

Table 8-2 DSA Object Classes Defined in ISP 15126-1

Ref. No.	Object Class	ATN DSA	Use in Asia/Pacific
1	ispApplicationEntity	o	N

Table 8-3 DSA Object Classes Defined in ISO/IEC ISP 11189

Ref. No.	Object Class	ATN DSA	Use in Asia/Pacific
1	mhs-distributionList	m	Y
2	mhs-message-store	m	Y
3	mhs-message-transfer-agent	m	Y
4	mhs-user	m	Y
5	mhs-user-agent	m	Y

Table 8-4 DSA Object Classes Defined by the ATN

Ref. No.	Object Class	ATN DSA	Use in Asia/Pacific
1	Atn-AmhsUser	m	Y
2	Atn-OrganizationalUnit	m	Y
3	Atn-OrganizationalPerson	m	Y
4	Atn-OrganizationalRole	m	Y
5	Atn-ApplicationEntity	m	Y
6	Atn-CertificationAuthority	m	Y
7	Atn-AmhsDistributionList	m	Y
8	Atn-AmhsUserAgent	m	Y
9	Atn-Gateway	m	Y
10	Atn-Aircraft	m	N
11	Atn-Facility	m	Y
12	Atn-AmhsMD	m	Y
13	Atn-IdrpRouter	m	Y
14	Atn-DirectorySystemAgent	m	Y
15	Atn-Organization	m	Y

Table 8-5 ATN Object Class and Attribute Contents in the ATN Directory

Object Class	Used in Asia/Pacific	Implementation Specified in 7.4		Data Population Specified by ASN.1	
Attribute		Mand.	Opt.	Mand.	Opt.
alias	Y	x			
aliasedEntryName	Y	x		x	
applicationEntity	Y	x			
commonName	Y	x		x	
description	Y	x			x
localityName	Y		x		x
organizationName	Y	x			x
organizationalUnitName	Y	x			x
presentationAddress	Y	x		x	
seeAlso	Y		x		x
supportedApplicationContext	Y		x		x
applicationProcess	O	x			
commonName	Y	x		x	
description	Y	x			x
localityName	Y		x		x
organizationalUnitName	Y	x			x
seeAlso	O,N		x		x
atn-AmhsUser (subclass of mhsUser)	Y	x			x
mhs-deliverable-content-length	Y		x		x
mhs-deliverable-content-types	Y		x		x
mhs-deliverable-eits	Y		x		x
mhs-message-store-dn	Y		x		x
mhs-or-addresses	Y	x		x	
mhsPreferredDeliveryMethods	Y		x		x
atn-PerCertificate	Y	x			x

Object Class	Used in Asia/Pacific	Implementation Specified in 7.4		Data Population Specified by ASN.1	
Attribute		Mand.	Opt.	Mand.	Opt.
atn-DerCertificate	Y	x			x
atn-extended-service-support	Y	x		x	
atn-amhs-direct-access	Y	x		x	
atn-AF-address	Y	x			x
atn-Cidin-mcf	N	x			x
atn-Ax-or-primary-Ax-address	Y	x			x
atn-secondary-Ax-address	Y	x			x
atn-ApplicationEntity (subclass of X.521 applicationEntity)	O	x			
commonName	Y	x		x	
description	Y	x			x
localityName	Y		x		x
organizationName	Y	x			x
organizationalUnitName	Y	x			x8
presentationAddress	Y	x		x	
seeAlso	O,N		x		x
supportedApplicationContext	Y		x		x
atn-facilityName	Y	x			x
atn-aircraftIDName	N	x			x
atn-PerCertificate	O,N	x			x
atn-DerCertificate	O,N	x			x
atn-version	Y	x			x
atn-CertificationAuthority	O,N	x			
authorityRevocationList	Y	x		x	
cACertificate	Y	x		x	
certificateRevocationList	Y	x		x	

Object Class	Used in Asia/Pacific	Implementation Specified in 7.4		Data Population Specified by ASN.1	
Attribute		Mand.	Opt.	Mand.	Opt.
commonName	Y	x		x	
crossCertificatePair	Y	x			
description	Y	x			x
destinationIndicator	Y	x			x
facsimilieTelephoneNumber	Y	x			x
localityName	Y	x			x
organizationalUnitName	Y	x			x
physicalDeliveryOfficeName	Y	x			x
postOfficeBox	Y	x			x
postalAddress	Y	x			x
preferredDeliveryMethod	Y	x			x
registeredAddress	Y	x			x
roleOccupant	Y	x			x
seeAlso	O,N	x			x
stateOrProvinceName	Y	x			x
streetAddress	Y	x			x
telexTerminalIdentifier	N	x			x
telexNumber	N	x			x
x121Address	Y	x			x
mhs-deliverable-content-length	Y		x		x
mhs-deliverable-eits	Y		x		x
mhs-message-store-dn	Y		x		x
mhs-or-addresses	Y		x		x
mhsPreferredDeliveryMethods	Y		x		x
mhs-deliverable-content-types	Y		x		x
atn-DirectorySystemAgent	Y	x			

Object Class	Used in Asia/Pacific	Implementation Specified in 7.4		Data Population Specified by ASN.1	
Attribute		Mand.	Opt.	Mand.	Opt.
commonName	Y	x		x	
description	Y	x			x
knowledgeInformation	Y	x			x
localityName	Y	x			x
organizationName	Y	x			x
organizationalUnitName	Y	x			x
presentationAddress	Y	x		x	
seeAlso	Y	x			x
supportedApplicationContext	Y	x			x
atn-PerCertificate	Y	x		x	
atn-DerCertificate	Y	x		x	
atn-Facility	Y	x			
locality	Y		x		x
country	Y		x		x
atn-FacilityName	Y	x		x	
atn-PerCertificate	Y	x			x
atn-DerCertificate	Y	x			x
atn-ApplicationEntityName	Y	x			x
atn-Aircraft	N	x			
country			x		x
atn-AircraftIDName		x		x	
atn-PerCertificate		x			x
atn-DerCertificate		x			x
atn-ApplicationEntityName		x			x
atn-OrganizationalUnit (subclss of organizationalUnit)	Y	x			

Object Class	Used in Asia/Pacific	Implementation Specified in 7.4		Data Population Specified by ASN.1	
Attribute		Mand.	Opt.	Mand.	Opt.
businessCategory	Y	x			x
description	Y	x		x	
destinationIndicator	Y		x		x
facsimileTelephoneNumber	Y	x			x
internationalISDNNumber	Y		x		x
localityName	Y	x		x	
organizationalUnitName	Y	x		x	
physicalDeliveryOfficeName	N	x			
postalAddress	N	x			
postalCode	N	x			x
postOfficeBox	N	x			x
preferredDelivery	Y		x		x
registeredAddress	N		x		x
searchGuide	N		x		x
seeAlso	N	x			x
stateOrProvinceName	N	x			x
streetAddress	N	x			x
telephoneNumber	N	x			x
teletexTerminalIdentifier	N		x		x
telexNumber	N		x		x
userPasssword	O		x		x
x121Address	Y		x		x
atn-facilityName	Y	x		x	
atn-version	Y	x			x
atnPerCertificate	N	x			x
atnDerCertificate	N	x			x

Object Class	Used in Asia/Pacific	Implementation Specified in 7.4		Data Population Specified by ASN.1	
Attribute		Mand.	Opt.	Mand.	Opt.
atn-Organization (subclass of organization)	Y	x			
businessCategory	Y	x			x
description	Y	x		x	
destinationIndicator	Y		x		x
facsimileTelephoneNumber	Y	x			x
internationalISDNNumber	N		x		x
localityName	N	x		x	
organizationalName	Y	x		x	
physicalDeliveryOfficeName	O	x			
postalAddress	O	x			
postalCode	O	x			x
postOfficeBox	O	x			x
preferredDelivery	O		x		x
registeredAddress	O		x		x
searchGuide	O		x		x
seeAlso	O	x			x
stateOrProvinceName	O	x			x
streetAddress	O	x			x
telephoneNumber	Y	x			x
teletexTerminalIdentifier	N		x		x
telexNumber	N		x		x
userPasssword	O		x		x
x121Address	Y		x		x
atn-facilityName	Y	x		x	
atn-version	Y	x			x

Object Class	Used in Asia/Pacific	Implementation Specified in 7.4		Data Population Specified by ASN.1	
Attribute		Mand.	Opt.	Mand.	Opt.
atnPerCertificate	Y	x			x
atnDerCertificate	Y	x			x
atn-AmhsDistributionList (subclass of distributionList)	O	x			
commonName	O	x			x
description	O	x			x
mhs-deliverable-content-types	O	x			x
mhs-deliverable-eits	O	x			x
mhs-dl-submit-permissions	O	x			x
mhs-or-addresses	O	x			x
mhs-PreferredDeliveryMethods	O	x			x
Organization	O	x			x
organizationalUnitName	O	x			x
owner	O	x			x
seeAlso	O	x			x
atn-amhs-extended-service-support		x		x	
atn-PerCertificate		x			x
atn-DerCertificate		x			x
atn-Cidin-mcf		x			x
atn-AF-address		x			x
atn-Ax-or-primary-Ax-address		x			x
atn-AmhsUserAgent (subclass of MHS User Agent)	Y	x			
commonName	Y	x		x	
presentationAddress	Y	x		x	
description	Y	x			x
localityName	Y	x			x

Object Class	Used in Asia/Pacific	Implementation Specified in 7.4		Data Population Specified by ASN.1	
Attribute		Mand.	Opt.	Mand.	Opt.
organizationName	Y	x			x
organizationalUnitName	Y	x			x
seeAlso	Y	x			x
supportedApplicationContext	Y	x			x
owner	Y	x			x
mhs-deliverable-content-length	Y	x			x
mhs-deliverable-content-types	Y	x			x
mhs-deliverable-eits	Y	x			x
mhs-or-addresses	Y	x			x
mhsUndeliverableEITS	Y	x			x
atn-amhs-extended-service-support	Y	x		x	
atn-AmhsGateway (subclass of atn-applicationEntity)	Y	x			
commonName	X.520	x		x	
description	x.520	x			x
localityName	X.520		x		x
organizationName	X.520	x			x
organizationalUnitName	X.520	x			x
presentationAddress	X.520	x		x	
seeAlso	X.520		x		x
supportedApplicationContext	X.520		x		x
atn-facilityName	ATN 7.5.3.8	x			x
atn-aircraftIDName	ATN 7.5.3.9	x			x
atn-PerCertificate	ATN 7.5.3.6	x			x
atn-DerCertificate	ATN 7.5.3.7	x			x

Object Class	Used in Asia/Pacific	Implementation Specified in 7.4		Data Population Specified by ASN.1	
Attribute		Mand.	Opt.	Mand.	Opt.
atn-version	ATN 7.5.3.11				
owner	X.402	x		x	
mhs-deliverable-content-types	X.402	x		x	
protocolInformation	X.402	x		x	
mhs-deliverable-classes	X.402	x		x	
atn-mtcu-characteristics	ATN	x		x	
atn-Ax-or-primary-Ax-address	ATN	x			x
atn-AF-address	ATN 7.5.3.1	x			x
atn-OrganizationalPerson (subclass of X.521 organizationalPerson)	Y	x			
businessCategory	Y	x			x
commonName	Y	x			x
description	Y	x			x
destinationIndicator	Y		x		x
facsimileTelephoneNumber	Y	x			x
internationalISDNNumber	N	x			x
locatlityName	Y	x		x	
organizationalUnitName	Y	x		x	
physicalDeliveryOfficeName	Y	x		x	
postalAddress	Y	x		x	
postalCode	Y	x		x	
postOfficeBox	Y	x		x	
preferredDeliveryMethod	Y	x		x	
registeredAddress	O,N		x		x
seeAlso	O,N	x			x

Object Class	Used in Asia/Pacific	Implementation Specified in 7.4		Data Population Specified by ASN.1	
Attribute		Mand.	Opt.	Mand.	Opt.
stateOrProvinceName	Y	x		x	
streetAddress	Y	x		x	
surname	Y	x		x	
telephoneNumber	Y	x		x	
teletexTerminalIdentifier	N		x		x
telexNumber	N	x			x
atn-facilityName	Y	x		x	
title	Y	x		x	
uniqueIdentifier	Y		x		x
userPassword	Y	x			x
x121Address	Y		x		x
mhsORAddressWithCapabilities	Y	x			
mhs-deliverable-content-length	Y		x		x
mhs-deliverable-content-types	Y		x		x
mhs-deliverable-eits	Y		x		x
mhs-message-store-dn	Y		x		x
mhs-or-addresses	Y	x			x
mhsPreferredDeliveryMethods	Y		x		x
mhsUndeliverableEITS	Y		x		x
atnPerCertificate	Y	x			x
atnDerCertificate	Y	x			x
generationQualifier	Y		x		x
givenName	Y		x		x
initials	Y		x		x
atn-OrganizationalRole (subclass of X.521 organizationalRole)	Y	x			

Object Class	Used in Asia/Pacific	Implementation Specified in 7.4		Data Population Specified by ASN.1	
Attribute		Mand.	Opt.	Mand.	Opt.
commonName	Y	x		x	
description	Y	x			x
destinationIndicator	Y		x		x
facsimilieTelephoneNumber	Y	x			x
localityName	Y		x		x
internationalISDNNumber	N		x		x
stateOrProvinceName	N		x		x
streetAddress	Y		x		x
organizationalUnitName	Y	x			x
physicalDeliveryOfficeName	Y		x		x
postOfficeBox	Y		x		x
postalAddress	Y		x		x
postalCode	Y		x		x
preferredDeliveryMethod	O,N		x		x
registeredAddres	Y		x		x
roleOccupant	Y	x			x
seeAlso	O,N	x			x
telephoneNumber	Y	x		x	
teletexTerminalIdentifier	N		x		x
telexNumber	N		x		x
x121Address	Y		x		x
atn-facilityName	Y	x		x	
atn-PerCertificate	Y	x			x
atn-DerCertificate	Y	x			x
mhs-deliverable-content-length	Y		x		x

Object Class	Used in Asia/Pacific	Implementation Specified in 7.4		Data Population Specified by ASN.1	
Attribute		Mand.	Opt.	Mand.	Opt.
mhs-deliverable-content-types	Y		x		x
mhs-deliverable-eits	Y		x		x
mhs-message-store-dn	Y		x		x
mhs-or-address	Y	x			x
mhsPreferredDeliveryMethods	Y		x		x
mhsUndeliverableEITS	Y		x		x
atn-AmhsMD	Y	x			
atn-global-domain-identifier	Y	x		x	
atn-icao-country-code	Y	x		x	
atn-IdrpRouter (subclass of device)	Y	x		x	
commonName	Y	x		x	
description	Y	x			x
localityName	Y		x		x
organizationName	Y	x			x
organizationalUnitName	Y	x			x
owner	Y	x			x
seeAlso	O,N		x		x
serialNumber	Y		x		x
atn-Net	Y	x		x	
atnPerCertificate	Y	x			x
atnDerCertificate	Y	x			x
atn-Version	Y	x			x
country	Y	x			
countryName	Y	x		x	
description	Y		x		x

Object Class	Used in Asia/Pacific	Implementation Specified in 7.4		Data Population Specified by ASN.1	
Attribute		Mand.	Opt.	Mand.	Opt.
searchGuide	O,N		x		x
device	O	x			
commonName	Y	x		x	
description	Y	x			x
localityName	Y		x		x
organizationName	Y	x			x
organizationalUnitName	Y	x			x
owner	Y	x			x
seeAlso	O,N	x			x
serialNumber	Y	x			x
dsa	Y	x			
commonName	Y	x		x	
description	Y	x			x
knowledgeInformation	O,N		x		x
localityName	Y		x		x
organizationName	Y		x		x
organizationalUnitName	Y		x		x
presentationAddress	Y		x		x
seeAlso	O,N		x		x
supportedApplicationContext	Y	x			x
group Of Names	N	x			
businessCategory	Y	x			x
commonName	Y	x		x	
member	Y	x		x	
description	Y	x			x

Object Class	Used in Asia/Pacific	Implementation Specified in 7.4		Data Population Specified by ASN.1	
Attribute		Mand.	Opt.	Mand.	Opt.
organizationName	Y	x			x
organizationalUnitName	Y	x			x
owner	Y	x			x
seeAlso	O		x		x
locality	Y	x			
description	Y		x		x
localityName	Y	x			x
searchGuide	O		x		x
seeAlso	O		x		x
stateOrProvinceName	Y	x			x
streetAddress	Y	x			x

9 Asia-Pacific Regional ATN Directory Services Profile

TBD

10 Asia-Pacific Regional ATN Directory Services Deployment Schedule

TBD

11 Recommendations

Members of the meeting are invited to review and provide comments on the ATN Directory Services Planning.