*International Civil Aviation Organization*

**THE FIFTH MEETING OF AERONAUTICAL TELECOMMUNICATION NETWORK (ATN) IMPLEMENTATION CO-ORDINATION GROUP OF APANPIRG (ATNICG/5)**

Kuala Lumpur, Malaysia, 31 May – 4 June 2010

**Agenda Item 9:** **Future use of DIRECTORY SERVICE**

# ATN DIRECTORY SERVICES

(Presented by United States of America)

**SUMMARY**

This paper conveys the summary of the Directory Service (DR) specified in the Asia/Pacific Directory Service and ICAO Doc. 9705 Aeronautical Telecommunication Network (ATN) Technical Manual. The DR is specified in ICAO Doc. 9705, which is soon to be consolidated into ICAO Doc. 9880, which is under consideration for implementation and operation within the Asia/Pacific Region, however, there are many issues that need to be addressed before the DR can be an effective operational tool.

# 1. INTRODUCTION

**1.1** Directory Services, which is based on the X.500 platform, allows users to collect information that describes users, applications, and other resources in a common directory that is accessible by all authorized users and applications within the Aeronautical Telecommunication Network (ATN).

**1.2** A Directory Service also provides an administrative tool to centrally managed information in a global ATN. Any updated information in the directory is immediately available to all users and directory-enabled applications. The definition of the directory service was completed and published as Sub-Volume VII of ICAO Doc. 9705 Edition 3. It defines the specific directory schema and the protocol subsets needed to store, retrieve, and use the associated entries.

**1.3** The primary reasons for implementing an ATN Directory to support AMHS operation are:

a) AFTN addresses are different from AMHS addresses, so the messaging gateways that connect AFTN and AMHS must translate between these different forms. The translation process depends on address translation data, which must be globally synchronized. The ATN Directory may be used to distribute, update and synchronize this address translation data.

b) To allow lookup and browsing of ATC object entries by operational and administrative staff.

c) It can support the Public Key Infrastructure required to provide digital signature security to AMHS and other applications

d) It will allow more efficient and timely management of much of the data required to operate the AMHS and the AFTN gateways.

**1.4** Many of the AMHS implementations that have already been actually commissioned by ANSPs (Air Navigation Service Provider) as yet do not use the AMHS Directory. There are several reasons for this:

a) The need for ATN Directory support when only a few ANSPs are actually connected using AMHS is low, because the AMHS can be managed relatively easily between pairs of ANSPs

b) Those ANSPs that have implemented AMHS want to get wider operational experience of the new AMHS technology before committing resources to implement the ATN Directory. However, as the number of interconnected ANSPs rises, the difficulties of management and co-ordination will grow exponentially, and will lead to a much more urgent requirement for support of the ATN Directory Services.

**1.5** The ATN Directory is a tool that may be configured to support many more ATC operational and administrative tasks. However, the AMHS use of the ATN Directory is the most immediate requirement. Once the ATN directory has been commissioned and set in operation for AMHS, it can be readily extended and used for further, non-AMHS/AFTN applications.

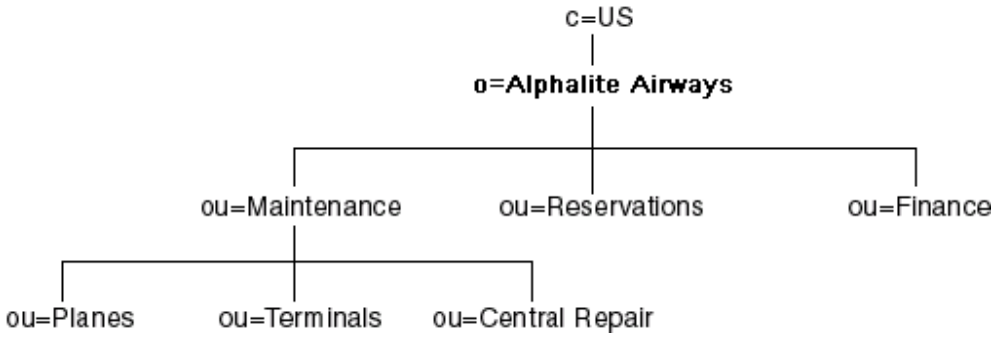
**1.6** The Air Traffic Service Messaging Management Center (AMC) has been in operation since 2009. Most of States have access to AMC to support the AMHS operation. The AMC is an “off-line” directory service that uses public internet while the DR is an “on-line” directory that uses ATN Internet. The AMC has addressed addressee’s coordination issues and centralized its operation into one center in Europe. However, other DR functions are left open.

## 2. DISCUSSION

### 2.1 Directory Structure

**2.1.1** The Directory Service (DS) database is distributed across directory servers called Directory Service Agents or DSAs. The DS data maintained by the DSAs are defined using a structure known as the Directory Schema. The information held by the 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 (DIT)

The following diagram shows an example of a DIT:




**2.1.2** The root of the tree is typically a country (C) followed by an organization (O). For example, in the figure above, the root of the tree is c=US, followed by an organization is o=Alphalite Airways. One or more organizational units (OU) typically appear below the root. These are *container* objects in that they can contain other directory entries. Directory entries that store information about a specific resource are referred to as *leaf* objects and they are added to the tree under an existing container object.

**2.1.3** The path to each entry in the tree is called its Relative Distinguished Name (RDN), and each RDN in the tree is unique. For example, using the DIT in the figure above, the RDN for the Airplane Maintenance Department of Alphalite Airways would be ou=Planes,ou=Maintenance,o=Alphalite Airways,c=US.

## 2.2 Directory Entries

A directory entry contains a set of name/value pairs, which are called attributes. An object class attribute is required for each entry in the directory. The object class determines which attributes are allowed for the entry as well as any??? that are required. The set of defined attributes and object classes that defines the content of acceptable entries within the directory server is called the Directory Schema.

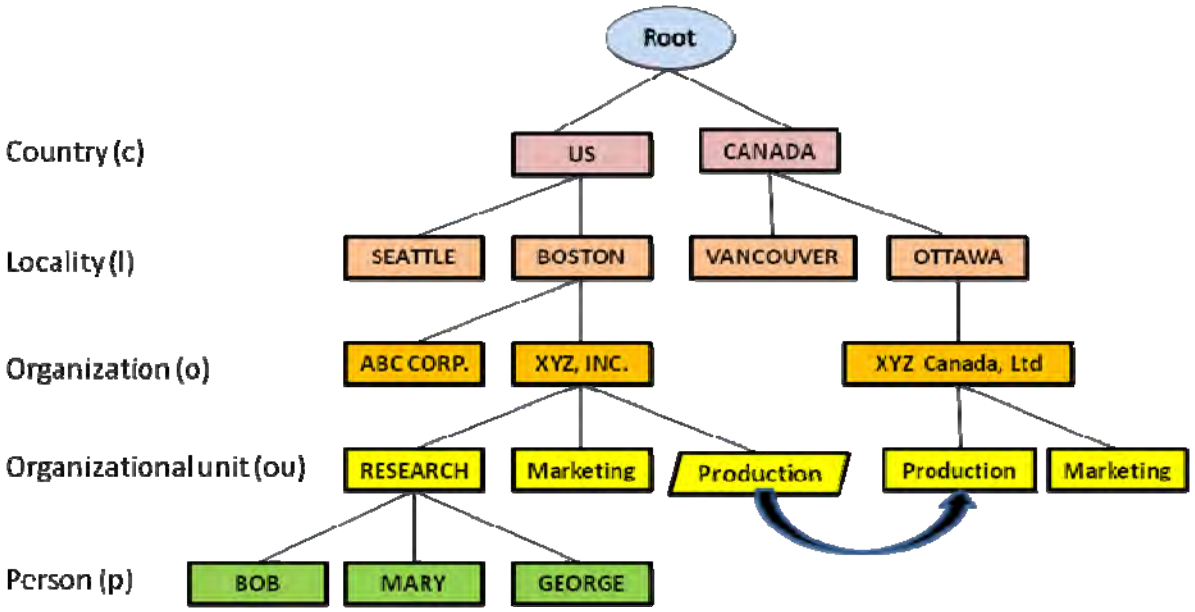



**Figure 2 –Directory Schema**

An attribute for a given entry may have multiple values. For example, because an OU can have multiple values assigned to it, a person might belong to more than one organization unit. When the DIT is searched, the order in which the attributes are returned cannot be guaranteed. Therefore, no implicit priority or hierarchy of attribute values can exist within an entry.

## 2.3 X.500 Directory Protocol Concepts

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

**2.3.2** A Directory System Agent (DSA) is the database in which the directory information is stored. This database is hierarchical in form, designed to provide fast and efficient search and retrieval. The DSAs are interconnected with the Directory Information Tree (DIT). The user interface program for access to one or more DSAs is a Directory User Agent (DUA).

**2.3.3** The Directory System Protocol (DSP) controls the interaction between two or more Directory Service Agents, and between a Directory User Agent and a Directory System Agent. This is done in such a way that an end user can access information in the Directory without needing to know the exact location of that specific piece of information.

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

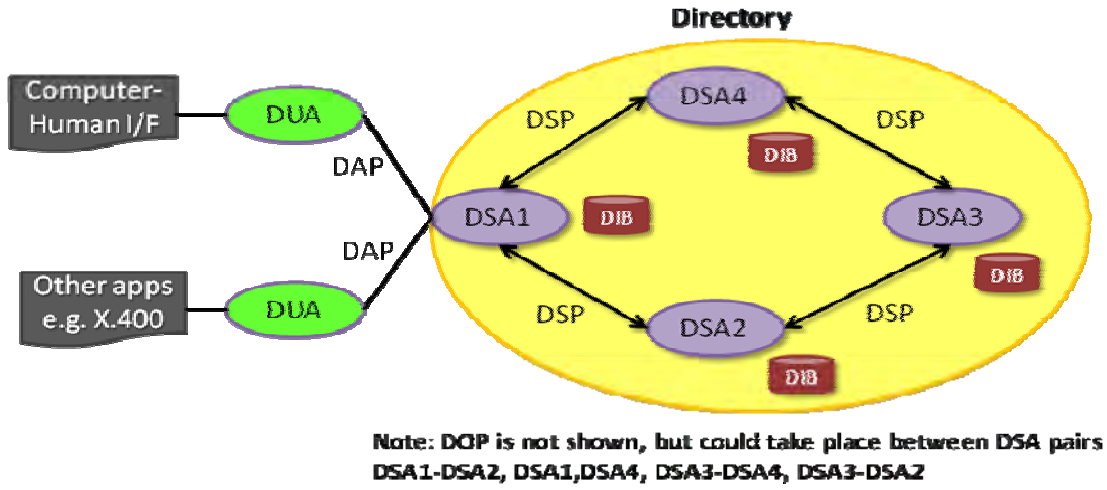



**Figure 3 –Directory Model**

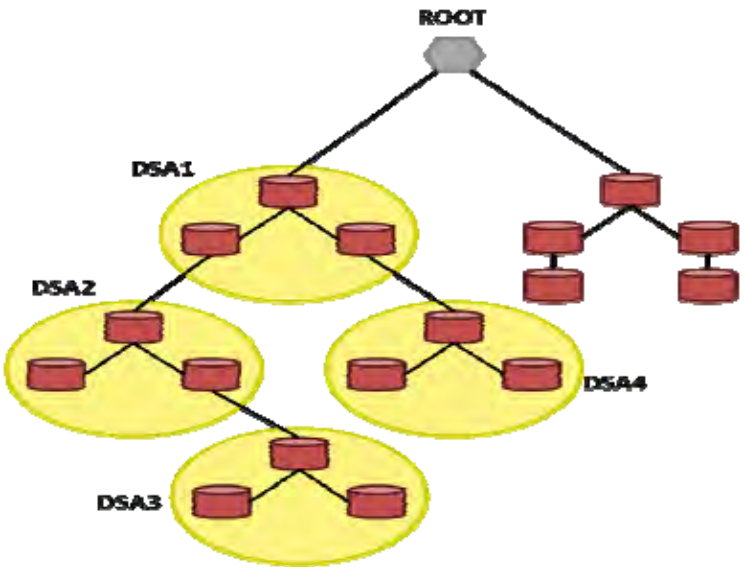



**Figure 4 –Directory Model Showing DSA**

The Directory concept is quite open and extensible:

- The objects may be persons, organizations, organizational units, computers, machines, countries etc. In the Air Traffic Control arena, special objects have been defined which include ACCs, aircraft, and ICAO States, reflecting Air Traffic Control requirements

- A set of Air Traffic Services attributes have been defined for use within the ATC Community. These include ACC Location codes, ATN Aircraft Identity, ATN Facility Identity, AMHS Addresses, and AFTN Addresses.

In fact, as with the 'Global Directory' envisaged by the ITU-T X.500 Recommendations, the ATN Directory is intended to be a global, distributed and possibly replicated database of ATN-specific object entries. This will allow each ANSP (Air Navigation Service Provider) to manage its own entries, while sharing and synchronizing those entries with other ANSPs.

## 3. SCENARIO

DUAs interact with the Directory by communicating with one or more DSAs. A DUA need not be bound to any particular DSA. It may interact directly with various DSAs to make requests. For some administrative reasons, it may not always be possible to interact directly with the DSA that needs to carry out the request. It is also possible that the DUA can access the Directory through a single DSA. For this purpose, DSAs will need to interact with each other. This specification applies to the initiator role of DAP within a DUA as shown in Figure 4.

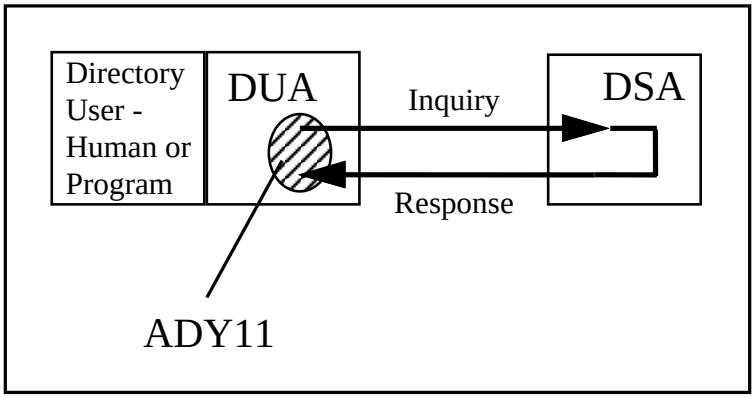



**Figure 4 – Access to the Directory**

DUA Support of Distributed Operations:

This section profiles the behavior of DUAs when Referrals or Search Continuation References are invoked by the DSA. A DUA creates an association to a DSA of its choice and invokes an operation. The DSA may return a referral instead of a result, or the result may contain continuation references. The latter occur

in the case of List or Search operations in which the DSA is unwilling or unable to complete the search, but is able to advise which other DSAs may be able to assist.

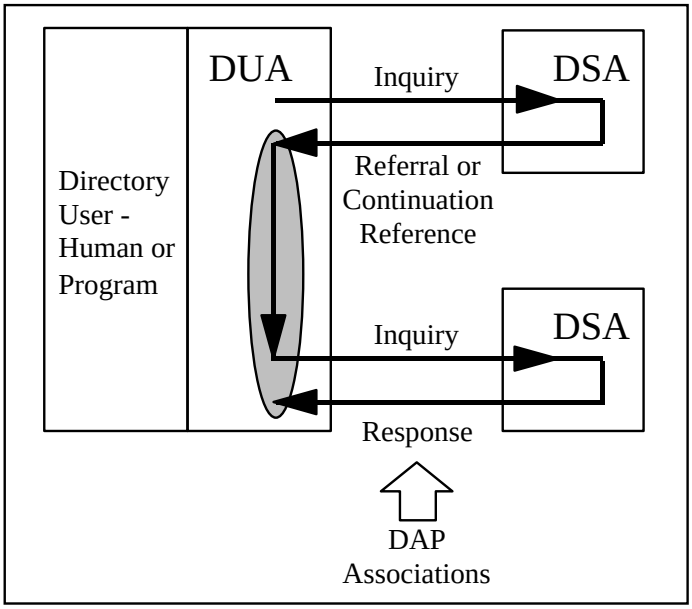



**Figure 5 – DUA Support of Distributed Operations**

## 3.1 Summary Requirements

The Table in this section lists all of the requirement differences between the Base Standards and the current specifications of SV7 DAP Protocol. These specifications contain many conditionals that are difficult to interpret. This summary proposes relevant requirements for the different DUA profiles.

**Requirement 1**: All ATN DUAs shall conform to all of the mandated requirements of the Base Standard specifications of the DAP Protocol.

**Requirement 2**: In addition, the following options of the DAP protocol are mandated for ATN DUA according to their intended use as given in the DUA profiles of section 3.2:

1. Strong Authentication for the DAP Bind Operation in both Initiator role and Responder role;
2. Strong Authentication for the DAP Bind Result in both Initiator role and Responder role;
3. Signed Read Operation and Signed Read Result;
4. Signed Compare Operation and Signed Compare Result;
5. Signed List Operation and Signed List Result;
6. Signed Search Operation and Signed Search Result;
7. Signed Add Entry Operation and Signed Add Entry Result;
8. Signed Remove Entry Operation and Signed Remove Entry Result;

9. Signed Modify Entry Operation and Signed Modify Entry Result;
10. Signed Modify DN Operation and Signed Modify DN Result;
11. DUA Support for the Distinguished Encoding Rules;
12. Support for Certificate Version 3;
13. Support for Certificate Revocation List Version 3;
14. Support for Authority Revocation List Version 3;
15. **Read Operation** – Modify Rights Request and Results for Entry, Attribute, Value and Permission;
16. **List Operation** – Paged Results; Name; Aliasentry; From Entry; QueryReference; UncorrellatedListInformation;
17. **Search Operation** – Subset; SearchAliases; PagedResults; ExtendedFilter; QueryReference; UncorrellatedsearchInfo;
18. **Modify Operation** – Removeattribute;
19. **Modify RDN Operation** – NewSuperior; Errors and Parameters (Abandoned, Abandonfailed, Attributeerror, Nameerror, Securityerror, Invalidsignature,Protectionrequired, Serviceerror, Invalidqueryreference, updateerror);
20. **CommonArguments** – SecurityParameters; OperationProgress; Referencetype; Entryonly; Exclusions; NameResolveonMaster;
21. **Common Elements** – SecurityParameters; Performer; Aliasdereferenced, ServicecontrolElements; Attributesizelimit; EntryInformationSelection; Attributes; AllUserAttributes; Select;
22. **Common Elements** – SecurityParameters; Performer;
23. **Entry Information Elements** – Fromentry; Information; AttributeType; Attribute; NonCompleteEntry;
24. **Filter Item Elements** – Equality; ExtensibleMatch;
25. **Paged Results Elements** – NewRequest; QueryReference;
26. **List Protocol Elements** – PartialOutcomeQualifier;
27. **Search Protocol Elements** – Referral;
28. **Common Arguments Protocol Elements** – OperationProgress; NameResolutionPhase; NotStarted; Proceeding; Completed; NextRDNtobeResolved;
29. **Continuation Reference Elements** – NextRDNtobeResolved; RDNsResolved; EntryOnly; ReturntoDUA; NameResolveonMaster;
30. **Supported References** – SelfReference; Superior Reference; ImmediateSuperiorReference; SubordinateReferen98; Non-Specific SubordinateReference;
31. **DUA Authentication – DAP Initiator** – Strong Authentication; Strong, Two Way Bind Request; Signed Operations; Strong Authentication – initiator; Strong Authentication – Responder; Common Algorithms; Generation of Certification path; V3 Certificate; V3 Certificate Revocation Lists; Authority Revocation Lists; Distinguished Encoding Rules;
32. **DUA Bind Elements** – Time1; Random1; CertificationPath; Name;
33. **DUA Bind Result Elements** – Time1; Random1; CertificationPath; Name.

### 3.2 Eight ATN DUA Profiles of the DAP Protocol

This section proposes eight different profiles for DUAs, each with different requirements within the ATN.

1. Directory Administrative DUA – The full ATN-DUA capability
2. Operational Personnel DUA (AMHS)
3. Operational DUA – AMHS MTA
4. Operational AMHS MTA – DUA
5. Operational AMHS UA – DUA
6. Operational AMHS MS – DUA
7. Operational AMHS MTCU – DUA
8. Non-Operational – DUA (All other ATN DIR users)

### 3.3 Directory Operations and Protocol Element requirements

The following Table specifies the Operations and Protocol Elements that shall be supported for the eight different types of ATN DUA. The values in the table represent the differences in the requirements of the Base Standard compared with the requirements of ATN DUAs. They are delta requirements. There is an implicit assumption that all of the mandated requirements of the Base Standard are inherited, and the requirements of the table are additional requirements of the ATN Directory. The values are derived from the ASN.1 notation of the base standards Abstract Service definitions in the following way:

- Where an ASN.1 operation or element is **not** marked as OPTIONAL in the base standard, its value is ‘m’. All ASN.1 productions supporting a mandated element, such a mandated element is also mandated unless they are declared as OPTIONAL.
- In the following table, the selected remaining OPTIONAL elements in the column ‘Protocol Element & Operation’ of the Base Standard ASN.1 are mandated for each of the eight different DUA Profiles. All supporting elements of each mandated option be also mandated.

| Protocol Element & Operation | Administrative DUA | Operational AMHS MTA - DUA | Operational AMHS UA – DUA | Operational AMHS MCTU | Operational DUA | Non-Operational DUA |
|---|---|---|---|---|---|---|
| Strong Authentication for the DAP Bind Operation in both Initiator role and Responder role | m | m | m | m | m | |
| Strong Authentication for the DAP Bind Result in both Initiator role and Responder role | m | m | m | m | m | |
| Signed Read Operation and Signed Read Result | m | m | m | m | m | |
| Signed Compare Operation and Signed Compare Result | m | m | m | m | m | |
| Signed List Operation and Signed List Result | m | m | m | m | m | |
| Signed Search Operation and Signed Search Result | m | m | m | m | m | |
| Signed Add Entry Operation and Signed Add Entry Result | m | | | | | |
| Signed Remove Entry Operation and Signed Remove Entry Result | m | | | | | |
| Signed Modify Entry Operation and Signed Modify Entry Result | m | | | | | |
| Signed Modify DN Operation and Signed Modify DN Result | m | | | | | |
| DUA Support for the Distinguished Encoding Rules | m | m | m | m | m | |
| Support for Certificate Version 3 | m | m | m | m | m | |

| Protocol Element & Operation | Administrative DUA | Operational AMHS MTA - DUA | Operational AMHS UA – DUA | Operational AMHS MCTU | Operational DUA | Non-Operational DUA |
|---|---|---|---|---|---|---|
| Support for Certificate Revocation List Version 3 | m | m | m | m | m | |
| Support for Authority Revocation List Version 3 | m | m | m | m | m | |
| **Read Operation** | **m** | **m** | **m** | **m** | **m** | **m** |
| Modify Rights Request and Results for | m | | | m | | |
| • Entry | m | | | m | | |
| • Attribute | m | | | m | | |
| • Value | m | | | m | | |
| • Permission | m | | | m | | |
| **List Operation** | **m** | | | | | **m** |
| • Paged Results | m | | | | m | m |
| • Name | m | | | | m | m |
| • Aliassentry | m | | | | m | m |
| • FromEntry | m | | | | m | m |
| • QueryReference | m | | | | m | m |
| • UncorrellatedListInformation | m | | | | m | m |
| • Search Operation | m | | m | m | m | m |
| • Subset | m | | | ? | m | m |
| • SearchAliases | m | | | ? | m | m |
| • PagedResults | m | | | ? | m | m |
| • ExtendedFilter | m | | | ? | m | m |
| • QueryReference | m | | | ? | m | m |
| • UncorrellatedsearchIfo | m | | | ? | m | m |

| | | | | | | |
|---|---|---|---|---|---|---|
| **Modify Operation** | m | | | | | |
| • Removeattribute | | | | | | |
| | m | | | | | |
| **Modify RDN Operation** | **m** | | | | | |
| • NewSuperior | m | | | | | |
| • Errors and Parameters (Abandoned, Abandonfailed, Attributeerror, nameerror, Securityerror, Invalidsignature,Protectionrequired, Serviceerror, Invalidqueryreference, updateerror) | m | m* | m* | m* | m* | m |
| **CommonArguments** | **m** | **m** | **m** | **m** | **m** | **m** |
| • SecurityParameters | m | m | m | m | m | ? |
| • OperationProgress | m | m | m | m | m | m |
| • Referencetype | m | m | m | m | m | m |
| • Entryonly | m | m | m | m | m | m |
| • Exclusions | m | m | m | m | m | m |
| • NameResolveonMaster | m | m | m | m | m | m |
| **Common Elements** | **m** | **m** | **m** | **m** | **m** | **m** |
| • SecurityParameters | m | ? | ? | ? | m | ? |
| • Performer | m | m | m | m | m | m |
| • Aliasdereferenced | m | m | m | m | m | m |
| • ServicecontrolElements | m | m | m | m | m | m |
| • Attributesizelimit | m | m | m | m | m | m |
| • EntryInformationSelection | m | m | m | m | m | m |
| • Attributes | m | m | m | m | m | m |
| • AllUserAttributes | m | m | m | m | m | m |
| • Select | m | m | m | m | m | m |

| | | | | | | |
|---|---|---|---|---|---|---|
| **Common Elements** | **m** | **m** | **m** | **m** | **m** | **m** |
| • SecurityParameters | m | ? | ? | ? | m | ? |
| • Performer | m | m | m | m | m | m |
| • Entry Information Elements | m | m | m | m | m | m |
| • Fromentry | m | m | m | m | m | m |
| • Information | m | m | m | m | m | m |
| • AttributeType | m | m | m | m | m | m |
| • Attribute | m | m | m | m | m | m |
| • NonCompleteEntry | m | m | m | m | m | m |
| **Filter Item Elements** | **m** | | | **m** | **m** | **m** |
| • Equality | m | | | m | m | m |
| • ExtensibleMatch | m | | | m | m | m |
| • Paged Results Elements | m | | | | m | m |
| • NewRequest | m | | | | m | m |
| • QueryReference | m | | | | m | m |
| **List Protocol Elements** | **m** | | | | **m** | **m** |
| • PartialOutcomeQualifier | m | | | | m | m |
| **Search Protocol Element** | **m** | | | **m** | **m** | **m** |
| • Referral | m | | | m | m | m |
| • Common Arguments Protocol Elements | m | | | | m | m |
| • OperationProgress | m | | | | m | m |
| • NameResolutionPhase | m | | | | m | m |
| • NotStarted | m | | | | m | m |
| • Proceeding | m | | | | m | m |
| • Completed | m | | | | m | m |
| • NextRDNtobeResolved | m | | | | m | m |
| | m | | | m | m | m |

| | | | | | | |
|---|---|---|---|---|---|---|
| • Continuation Reference Element | m | | | m | m | m |
| • NextRDNtobeResolved | m | | | m | m | m |
| • RDNsResolved | m | | | m | m | m |
| • EntryOnly | m | | | m | m | m |
| • ReturntoDUA | m | | | m | m | m |
| • NameResolveonMaster | | | | | | |
| **Supported References** | **m** | **m** | **m** | **m** | **m** | **m** |
| • SelfReference | m | ? | ? | ? | m | m |
| • Superior Reference | m | m | m | m | m | m |
| • ImmediateSuperiorReference | m | ? | ? | ? | m | m |
| • SubordinateReference | m | m | m | m | m | m |
| • Non-Specific SubordinateReference | m | m | m | m | m | m |
| **DUA Authentication –DAP Initiator** | **m** | **m** | **m** | **m** | **m** | |
| • Simple | m | | | | | m |
| • Strong Authentication | m | m | m | m | m | m |
| • Strong | m | m | m | m | m | m |
| • Two Way Bind Request | m | m | m | m | m | m |
| • Signed Operations | m | m | m | m | m | m |
| • Strong Authentication-initiator | m | m | m | m | m | m |
| • Strong Authentication-responder | m | m | m | m | m | m |
| • Common Algorithms | m | m | m | m | m | m |
| • Generation of Certification path | m | m | m | m | m | m |
| • V3 Certificate | m | m | m | m | m | m |
| • V3 Certificate Revocation Lists | m | m | m | m | m | m |
| • Authority Revocation Lists | m | m | m | m | m | m |
| • Distinguished Encoding Rules | m | m | m | m | m | m |
| **DUA Bind Elements** | **m** | **m** | **m** | **m** | **m** | **m** |

| | | | | | | |
|---|---|---|---|---|---|---|
| • Time1 | m | m | m | m | m | m |
| • Random1 | m | m | m | m | m | m |
| • CertificationPath | m | m | m | m | m | m |
| • Name | m | m | m | m | m | m |
| **DUA Bind Result Elements** | **m** | **m** | **m** | **m** | **m** | **m** |
| • Time1 | m | m | m | m | m | m |
| • Random1 | m | m | m | m | m | m |
| • CertificationPath | m | m | m | m | m | m |
| • Name | m | m | m | m | m | m |

## 4. CONCLUSION

The meeting is invited to consider the information presented in this paper. It is recommended that the ATNICG consider an additional activity to the DR Task to perform the followings:

1. Analyze AMC functions that overlap DR functions
2. Analyze and recommend near term and long term DR functions that can be implemented
3. Analyze and specify if an operational procedure is required for DR
4. Indentify and specify obstacles to implementing DR service

It is further recommended that the first report to be presented at the ATNICG WG/8 to be held in September 2010.