EUROCONTROL

ATNP/WG3/WP **17-14**

20 September 1999

AERONAUTICAL TELECOMMUNICATION NETWORK PANEL

WORKING GROUP 3 (APPLICATIONS AND UPPER LAYERS)

Gran Canaria, Spain, 28 September - 1 October 1999

Agenda Item 6.4: ULCS Post Package 1 work

ATN Directory Considerations

Prepared by: David Eadsforth

Presented by: Tony Kerr

SUMMARY

This paper considers issues arising from the Draft Sub-Volume 7 (Directory Services) of the ATN Technical Provisions. It is concluded that there are several issues, mostly non-technical in nature, which need to be addressed before a Directory system can be successfully deployed.

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Background

The document **DRAFT SUB VOLUME 7 - DIRECTORY SERVICES**, dated May 19, 1999, has been issued in response to the specific requirements of the WG3 AMHS sub-group and the WG1 security sub-group of the Aeronautical Telecommunication Network Panel (ATNP). The document defines those protocols and services believed necessary if the participants in the ATN are to be able to exchange directory data.

Although this is an incomplete draft, the body of the document reveals clearly the direction of the author's thinking, and there is no reason to doubt that the final version of the document will adequately cover the perceived technical requirements for data exchange. However, it has to be said that a document containing subject matter such as this would normally be issued at the end of a preliminary process, which would be designed to discover all potential critical user business requirements.

1.2 Purpose of this Paper

This document is intended to highlight a number of directory issues which may be pertinent to this situation, and which may form the basis for discussion. There may be an opportunity to take action to discover and clarify a number of user requirements that may not have been fully expressed to date.

These considerations for the creation of a directory service for a distributed user community are based on experience of the actual deployment of such a service.

2. THE CONCEPT OF A DIRECTORY SERVICE

It may be useful to consider the basic purpose of a directory service. The effectiveness of any service can only be assessed in relation to the degree to which it meets the perceived requirements. In the case of a directory service, key questions will include:

1. Who (or what function) is to use the service?
2. What end-user functionality will be required?
3. What will be the pattern of use?
4. What underlying support functions will the directory service have to perform (by implication, in a manner transparent to the end user) to provide the correct information to the end user in a consistent and reliable fashion?

This last question hints at one fundamental aspect of directory operation; to what degree is the directory facility to be a fully supported service? It is possible to provide users with a basic directory facility that enables them to search for information about other users, but this could simply be a flat file on a LAN server, for example (and indeed, some simple directory products are little more than that), with information limited in both content and coverage. On the other hand, a directory facility might have a highly complex architecture capable of providing anything from basic information about local users to extensive, fully managed and supported global links to other directories, and also feature sophisticated browsing and search. It is the versatility of the user requirement that will ultimately define the complexity of the underlying directory service, and this is the direction from which the design of a community directory service should be derived.

It is appreciated that sometimes an implementation schedule may not permit a full study of end user requirements before some form of directory interworking has to be put in place. However, a sufficient appreciation of end user requirements can usually be made to permit a strategy for a community directory service to be defined so that all participants know what the final aims are to be, and can then gear their plans to the common aim

without omitting vital steps along the way, or even taking a completely different direction to other participants.

3. DIRECTORY TOPOLOGY

ATN organisations share a number of the challenges that face international military organisations, for instance NATO. Such organisations have, for example, to control the activities of a large number of vehicle fleets, and to do so safely, in the presence of a number of threats to the operation. Operational communications and supporting services (like Directory) have to run smoothly at all times and have to possess a higher degree of resilience than those of most civil organisations.

Thus a number of fundamental issues face the participants of the ATN in the creation of a community directory service. Although a robust standard (X.500) may have been selected as the common protocol and service interface between participants, there is still much to decide in the area of how the participants' data is to be managed, that is to say assembled, made available, accessed, updated, and continually supported.

The most basic topology that would be likely to be considered for a community directory service would be that each organisation would undertake to create an X.500 Directory Service Agent (DSA) and associated Directory Information Base (DIB) that would contain mutually agreed data. However, even such a basic topology raises a number of issues:

1. Will each national directory hold information solely about its own community, or should directories cache copy or shadow (even partially) the information held in the directories of other national communities for purposes of performance or availability?

2. What is the scope for the use of chaining and referral techniques, and to what depth should each national service be expected to support these?

3. Should each nation be permitted to update content (and if so, what?) in other participants directories?

4. Should directory content be mastered wholly by each participant or should there be a central master directory which is guaranteed to be kept up to date, and from which participants may draw particular content into their own directories?

5. Should the sharing and modification of directory content be controlled by each participant adhering to a set of rules, with overall control being exercised by no-one in particular, or should the participants set up some kind of management organisation which would carry out all support activity, and in so doing probably minimise the possibilities of errors and unavailability?

It is noteworthy that the Allied Command Europe Rapid Reaction Corps (ARRC), faced with the difficulty of linking together the command and control functions of many nations, decided to give the responsibility of implementing the communications network for deployed forces to one organisation. The resulting system was the Interim ARRC Information System, which provides the network infrastructure, messaging, and directory facilities to the ARRC. While the ATN participants may not wish to select an individual nation as such to perform a similar role, it should be possible to create an organisation that could manage the core of such shared facilities.

The draft Sub-Volume 7 makes no reference to topology issues. It merely lists a selection of profiles for directory access, chaining and referrals and it is implicit that all ATN organisations are required to deploy all elements - Directory User Agents (DUAs) and DSAs - to comply with the provisions of the Sub-Volume.

4. DIRECTORY CONTENT

What should go into a directory can be the source of endless debate, nevertheless, directory content will have to be debated fully by the participants to ensure that all useful items are present. As a general rule, it is probably safer to include a debatable item rather than exclude it.

4.1 Naming Conventions

One subject that could be usefully investigated is the question as to whether the standardisation of names will be of benefit. This is an area that has been the subject of study by the military, with the conclusion that standardisation can be highly useful. For example, if a staff officer in a headquarters wishes to look up the rolename of someone in another headquarters, it is useful to have a starting point in the way of a deducible naming structure. Thus instead of having to study a file of directory entries, or spend too much time browsing different views of the directory data, a search can be made for a standard title which will have a high probability of hitting the desired entry first time.

As noted earlier, the roles of the civil aviation organisations of the world have similarities with those of military organisations, and the roles of ATC staff around the world probably feature a high degree of equivalence. It would probably be of great benefit operationally if the Common Names in the directories were deducible and could be eligible for generic search.

4.2 Directory Views

Much debate can be expended on the question of what options should be chosen for the access and display of directory data. As previously mentioned, some existing proprietary products can be very simple, little better that flat files. At present, X.500 still appears to offer the most flexibility for storage and access of directory data, and an X.500 User Agent still appears to offer the most features to the end user.

One feature of directories that most users find highly valuable is the ability to browse directory data from different viewpoints. If directory data can displayed for instance, organisationally, geographically, and perhaps in other ways, the users stand the best chance of finding the entries they are looking for. Such an arrangement can be arrived at by having one physical directory database structure and then using the Alias function to generate the alternative views.

If participants are using proprietary directory products, and are limited to the kind of searches that can be generated by such products, and then having these translated and transferred to an X.500 environment, then some of these operations, such as browsing different views of the data, may not be possible.

End users who could be identified as having a critical need for particularly versatile directory access should be considered as eligible for a full function X.500 User Agent, so that such advanced facilities may be made available.

During periods of operational stress, when it may be necessary to locate entries in the shortest possible time, a powerful directory User Agent could be welcome, if not vital. However, the proposal in the draft Sub-Volume 7 is to make no use the ATN Security Label, which would result in Directory traffic being treated as General Communications, and potentially queued behind low-priority bulk data.

5. SUMMARY

This paper has not sought to provide in-depth planning detail on the X.500 directory implementation process. It has attempted to focus on what might be viewed as some critical similarities between the directory requirements of the ATN and analogous military directory systems, since these point to what should be some fruitful areas of investigation. In particular, it is suggested that the following be considered:

a) Confirmation of the critical functions to be supported by the core group of X.500 Directory Service Agents supplied by the participants, and thus the supporting protocols (i.e. DISP, DOP, DSP).

b) Consideration of the option to place the management and support of the core group of X.500 DSAs under a single management organisation. In fact, if such facilities as Certificate Authorities and Certificate Revocation Lists are to be used, then an organisation which can exercise at least some form of central management may be necessary.

c) Role based Common Names to reflect operational functions.

d) The use of Aliases to provide different views of Directory data.

e) Provision of native X.500 User Agents to end users with critical operational requirements.

The draft Sub-Volume 7 requires conformance to several International Standardised Profiles, which in turn profile a number of complex OSI protocols. As noted in a previous paper (WG3/WP16-13 “Directory Protocol Requirements for ATN Deployment”), it would be a very onerous requirement if all ATN participants were mandated to procure, configure, operate and maintain a full X.500 Directory infrastructure.

The above considerations lead to the following conclusions:

a) A Concept of Operations for the deployment of Directory systems by ATN organisations is urgently needed, and should address some of the issues raised in this paper.

b) Careful consideration should be given to the full implications before States and Organisations who implement ATN are mandated to operate an X.500 infrastructure internally.