EUROCONTROL

ATNP/WG3/WP **16-13**

12 May 1999

AERONAUTICAL TELECOMMUNICATION NETWORK PANEL

WORKING GROUP 3 (APPLICATIONS AND UPPER LAYERS)

Naples, Italy, 18 - 21 May 1999

Agenda Item 11: Any Other Business

Directory Protocol Requirements for ATN Deployment

Prepared by: Tony Kerr

Presented by: Tony Kerr

SUMMARY

This paper raises the question of the degree of support for standardised Directory protocols which is required for the successful operation of an ATN infrastructure. The specification of such protocols is not on the current WG3 work programme. Nor is Directory explicitly on the work programme of WG1. The Working Group is invited to consider the issues raised and decide how to proceed.

1. INTRODUCTION

1.1. Scope

This paper considers the need for standardised directory protocols in the ATN environment. This results from an action item from WG3's 15th meeting in Honolulu to look at some of the issues specifically related to X.500 protocols (as opposed to the Directory information model and Schema).

The objective is to stimulate discussion on the need (or otherwise) for ICAO SARPs material (or Technical Provisions) requiring ATN participants to implement a standard directory infrastructure and related policies.

1.2. References

[1] ISO/IEC 9594-1/7: 1995 Data Communication Networks - The Directory (see also ITU-T X.500:1995 Series)

[2] ISO/IEC ISP 10616:1995 - Information Technology - International Standardized Profile FDI11 - Directory Data Definitions - Common Directory Use (Normal)

[3] ISO/IEC ISP 11189 - Information Technology - International Standardized Profile FDI2 - Directory Systems - MHS Use of Directory

[4] ISO/IEC 9594-8 Information technology - Open systems interconnection - The Directory : Authentication Framework (ITU-T Recommendation X.509)

[5] ATNP WG3/WP15-29 The use of X.500 protocols in ATM Data Link Technology : ATN Directory Approach, G. Saccone.

[6] ATNP WG3/WP11-16 AMHS Directory Requirements and Specification Approach, J-M Vacher

2. BACKGROUND

A general Directory Schema is currently under development as Sub-Volume 7 of the ATN Technical Provisions. This will support, as a minimum, the storage of information which will satisfy AMHS requirements and security certificate (X.509) requirements.

However, the OSI Directory is much more than just the Schema. It is physically a global interlinked system, comprising:

Directory System Agents (DSAs), which store all or parts of the schema, and which communicate via the standard Directory System Protocol (DSP) to ensure that requirements for data replication, distribution and currency are met. Requests for information from a DSA may be answered directly by that DSA, automatically "chained" to another DSA, or the requester may just be referred to another DSA.

Directory User Agents (DUAs), which provide users with reliable access to the global Directory system via the standardised Directory Access Protocol (DAP).

The DSP and DAP are full 7-layer OSI protocols, specified to utilise the connection-oriented OSI Transport Service. There are "lightweight" variants of the DAP in widespread use, such as LDAP, and the ITU-T profile for X.500 over TCP/IP.

In ATNP, a working paper [6] was presented to the 11th meeting of Working Group 3 (Redondo Beach, Oct 1997). Extracts from the meeting report state: "It was recognised there that Directory Services did not fit neatly into an individual sub group and that clearly all WG3 sub groups would be involved. The

group was advised that the ATNP/2 report stated that X.500 services are to be integrated with GM and ATSMHS. It was recognised that an overall picture of the requirements and possible solutions was needed before making any decision on the subject. The Rapporteur stressed the need that all sub groups make swift progress on this task."

SG3 at its Toulouse meeting in January 1999 concluded that there are no known Package 2 requirements for Directory protocol (DAP, DSP) SARPs - to be confirmed by WG3. The issue may need to be revisited in the light of current developments in security, AMHS, and other ATN applications.

The report of the 15th meeting of WG3 (Honolulu, Jan 99) indicates that X.500 protocols will be included in a future version of WP15-29 [5].

3. DISCUSSION

Within ATNP, no significant work has been performed to date on the specification or profiling of directory protocols for the ATN environment.

The first requirement is for storage of information, which needs a standardised Schema definition. Then it follows that a protocol is needed to access the information. There are no specific requirements identified to date for a standardised protocol.

However, in some cases, such as considerations of Public Key Infrastructure for ATN security, or address look-up for AFTN/AMHS Gateways, the existence of a global, interconnected ATN directory is almost taken for granted.

Within WG3/SG3, it is acknowledged that the current security concept requires X.509 certificates. However, it does not require X.500 per se. Security mechanisms do not mandate X.500 protocols, but security discussions often assume that a global ATN Directory will exist.

The issue to be resolved is: to what extent are Directory protocols mandated for Package 2?

If Directory protocols are mandatory for future ATN operation, work must start urgently to specify Directory profiles to work over ATN Internet.

What is the operational concept? Is a profile needed for the exchange of Directory information between Administrations? WG1 input is needed.

AMHS refers to Directory ISPs - MHS use of Directory [3]. What are the implications for a supporting comms stack? See Annex A.

Whilst off-the-shelf Directory products are readily available, they would require some level of customisation to operate over the ATN Internet Communications Service. It would be a very onerous requirement if all ATN participants were mandated to procure, configure, operate and maintain a full Directory infrastructure.

There are also policy issues to consider, relating to the distribution of Directory subtrees between systems, the frequency of synchronisation updates, optional support for chaining, referral, etc.

What security provisions would be required, in terms of access control, authentication and integrity?

4. RECOMMENDATION

It is recommended that WG3 discuss the issues raised in this paper in order to reach a definitive position on the requirements for Directory protocol standardisation for ATN. If necessary, WG1 should be asked to clarify the concept behind the use of X.500 Directory in the areas indicated.

ANNEX A: USE OF DIRECTORY FOR AMHS

The following text is adapted from ATNP WG3/WP11-16 -AMHS Directory Requirements and Specification Approach, by J-M Vacher (Oct 1997).

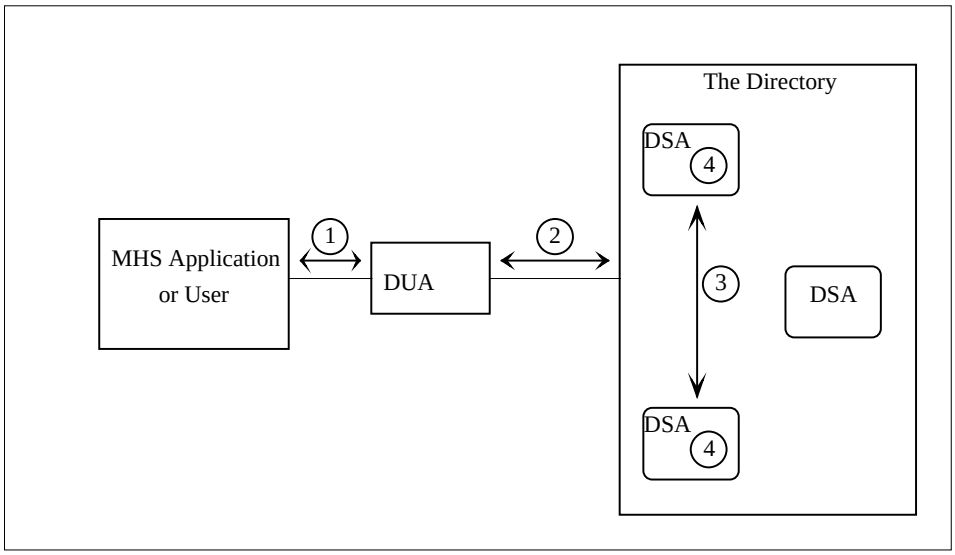
WP11-16 provided a first analysis of the requirements for Directory Services in support of AMHS. It also presented the ISO Profile for MHS Use of Directory (ISO/IEC DISP 11189, also known as FDI2).

The paper recommended an approach for the specification of the ATN Directory in support of AMHS, which includes the mandatory support of FDI2 and of the Distribution List (DL) functional group of FDI2. It also identified a number of areas to be further studied to progress such specification.

The SG1 Work Programme includes several items related to Directory Services, either in a manner dedicated to ATS Message Handling Services, or in a general manner not restricted to a ground-ground ATN application but covering potentially the entire ATN requirements for Directory Services.

Figure 1 depicts the general scenario by which an MHS application, by means of its associated DUA, obtains Directory information by accessing directly or indirectly one or more DSAs of the Directory.

Figure 1: MHS use of the Directory scenario



DUA = Directory User Agent
DSA = Directory System Agent

1: interface or protocol between user and DUA
2: protocol for access to the Directory (DAP)
3: protocol for exchanges between DSAs (DSP)
4: information held by DSAs

In the specification of the Directory in support of AMHS, items 1 to 4 of Figure 1 may be specified. WP 11-16 addressed only the issue of the information to be held in ATN Directory System Agents (DSAs) for use by AMHS Systems, i.e. item 4 of Figure 1.

Other elements in the specification should be the subject of further work, as suggested below.

The considered ATN DSAs may either:

- be dedicated to the AMHS Directory; thus being "AMHS DSAs"; or
- be part of the overall ATN Directory and thus retaining further information as required by other ATN end systems and/or intermediate systems.

A.1 Overview of FDI 2 (MHS Use of Directory) ISO ISP

ISO/IEC have published several International Standardised Profiles (ISPs) relatining to the OSI Directory standards. Profiles denoted “FDI” are concerned with information representation and encoding, whilst

profiles denoted “ADI” are concerned with communication protocols in the OSI Session, Presentation and Application layers.

Profile FDI 11, published as ISO/IEC ISP 10616 [2], profiles information to be stored in the Directory which is common to a variety of applications.

The FDI 2 profile, as specified in ISO/IEC ISP 11189 [3], augments this with specific information for use with Message Handling Systems. This specific information which may be supported in relation with Message Handling Systems is itself specified in the MHS base standards, namely in Annex A of ISO/IEC 10021-2. The FDI 2 profile explicitly refers to this annex.

The primary objective of FDI 2 is to define the minimum capabilities that Directory System Agents (DSAs) must have, to support an MHS application's view of Directory information. It does this by specifying a minimum set of structure and naming elements for the Directory Information Tree (DIT) which a DSA must be capable of holding and accessing, and other minimum schema requirements.

The FDI 2 profile does not limit DSAs to these minimum capabilities. The implementation of additional information handling (storage, retrieval and modification) capabilities is encouraged, but not mandated as this is not in the scope of the considered ISP.

Like many other ISPs, the FDI 2 profile specifies basic requirements and optional functional groups (FGs). The meaning of such concepts is identical to that of, e.g. MHS ISPs; however the way it applies is slightly different due to the different context. Three FGs are defined in FDI 2:

- the Distribution List (DL) Functional Group,
- the Additional Matching Rules (AMR) Functional Group, and
- the Substring Matching Rules (SMR) Functional Group.

The scope of FDI 2 is limited to the elements above. This means that it does *not* address, for example, the protocols used by a Directory User Agent (DUA) to access and retrieve information from DSAs. Neither does it address the relationship between the MHS Application or user and the DUA.

A.2 Applicability to the ATN and ATSMHS environment

A.2.1 Directory requirements in support of AMHS

Since WP11-16 was mostly related to the potential use of the FDI 2 profile in the ATN environment, only the AMHS was considered in this analysis. FDI 2 is neither applicable to the ATN Pass-Through Service, nor to other ATN applications.

In a first instance, the following requirement is considered as mandatory in support of the AMHS, when considering Directory Services:

- Determination of an AMHS user's O/R-Address from its directory name, and from an alias which would be its AF-Address if existing.

Again in a first approach, although not strictly mandatory, the following requirements may be considered as useful good practice in support of the AMHS, when considering Directory Services:

- storing and retrieving information on DLs for DL-expansion (list of dl-members, etc.);
- MHS user capability assessment (deliverable content length, etc.);
- determination of information about the application entities supporting MTAs (ATS Message Servers), MSs (if any) and ATS Message User Agents (UAs). Such information may include for example addressing information.

These functions may also be achieved by other implementation solutions, such as local tables for example. However, if a Directory Service is to be implemented, e.g. to meet the mandatory name

resolution requirement, it seems logical to use the same Directory as a standard technical means of implementing the functionalities above.

These requirements are summarised in Table 1, together with the AMHS Systems to which they are applicable.

Table 1: List of Directory requirements in support of AMHS

Reference	Requirement	Level	Applicable to
R1	Determination of an AMHS user's OR-Address from its directory name, and from an alias being its AF-Address	Mandatory	AFTN/AMHS Gateway
R2	Determination of an AMHS user's OR-Address from its directory name, and from an alias being its AF-Address	Optional	ATS Message User Agent
R3	Storing and retrieving information on DLs	Recommended (good practice)	ATS Message Server
R4	MHS user capability assessment	Recommended (good practice)	ATS Message Server
R5	Determination of information about the application entities supporting MTAs, MSs and UAs.	Recommended (good practice)	ATS Message Server

A.2.2 Adequacy of FDI 2 to meet the AMHS requirements for Directory Services

In the ISO/IEC and ITU-T environments, the FDI 2 profile has been designed to meet the requirements above, as far as the information to be held is concerned. Apart from the AMHS specifics (such as the use of AF-Address as an alias), it is supposed to fulfil the requirements placed on a DSA for this purpose.

Additionally, since support of the DL functional group of the MHS ISPs has been made mandatory in the ATSMHS SARPs, it is suggested to adopt the same approach as far as Directory is concerned.

As stated in the general description of FDI 2, only the minimum set of information to be held in the Directory Information Tree (DIT) is specified in this profile, without precluding the implementation of additional capabilities. In the ATN environment, this allows a DSA supporting the AMHS not to be restricted to this environment, and to be possibly used for other purposes. However, a DSA claiming "general support of the ATN", including AMHS, would need to conform to FDI 2.

A.3 Proposed approach

The following approach was proposed in WP11-16, for the specification of the Directory Services in support of AMHS to be included in a future CNS/ATM SARPs package:

1. mandate the support of the basic requirements of Profile FDI 2, as specified in ISO/IEC ISP 11189;
2. mandate the support of the DL Functional Group of Profile FDI 2;
3. investigate if the support of other object classes or attribute types is required, and should therefore be made mandatory, to fulfil the expressed requirements in support of AMHS, including the specific

requirements of AMHS (support of AF-Addresses). Such support would be required from ATN DSAs, for use by AFTN/AMHS Gateways and possibly ATS Message User Agents;

4. investigate if the support of the Additional Matching Rules (AMR) or Substring Matching Rules (SMR) is required, and should therefore be made mandatory (e.g. to help from AF-Address to/from MF-Address conversion). Such support would be required from ATN DSAs, for use by AFTN/AMHS Gateways and possibly by ATS Message User Agents;
5. investigate the requirements to be placed on the AMHS applications obtaining information from the ATN Directory. The related AMHS applications are the ATS Message Server, the AFTN/AMHS Gateway and possibly the ATS Message User Agent;
6. investigate the requirements to be placed on the DUAs associated with such AMHS applications. *This work should include an analysis of the suitability of the ISO/IEC ADInn Profiles to the AMHS environment.*

A.4 Conclusions

The Working Group was invited:

1. to endorse the approach adopted by SG1,as described above;
2. if the ATNP Working Groups jointly adopt an integrated strategy for an overall ATN Directory, to report to any other appropriate ATNP working group, that the specification for such ATN Directory should satisfy items 1 and 2 of this approach;
3. to note that SG1 intends to further refine the study of requirements and analysis of the Directory ISPs, in order to progress the investigation identified in items 3 to 6 of the proposed approach;
4. *to analyse the suitability of ISO/IEC Profiles ADInn and FDI 11 for the specification of the Directory in the overall ATN environment.*