ISTITUTO NAZIONALE DI FISICA NUCLEARE

Centro Nazionale Analisi Fotogrammi

INFN/TC-95/01
3 Gennaio 1995

P. Bonetti, G. Vita Finzi:

THE DIRECTORY SERVICE X.500 IN I.N.F.N.

SIS-Pubblicazioni
dei Laboratori Nazionali di Frascati

INFN - Istituto Nazionale di Fisica Nucleare
Centro Nazionale Analisi Fotogrammi

INFN/TC-95/01
3 Gennaio 1995

THE DIRECTORY SERVICE X.500 IN I.N.F.N.

P. Bonetti, G. Vita Finzi
INFN–CNAF, Viale Ercolani 8, I–40138 Bologna

Abstract

This report describes the deployment of the Directory X.500 in INFN to provide a White Pages Service. After a short introduction on the Standard, we briefly explain the logical structure of the database and its implementation in a UNIX environment using TCP/IP network protocols. Many user interfaces, either for VMS, UNIX or Macintosh are here described, togheter with gateways to other information systems, such as WWW and Gopher. Some of the tools have been developed at INFN-CNAF.

1. - INTRODUCTION

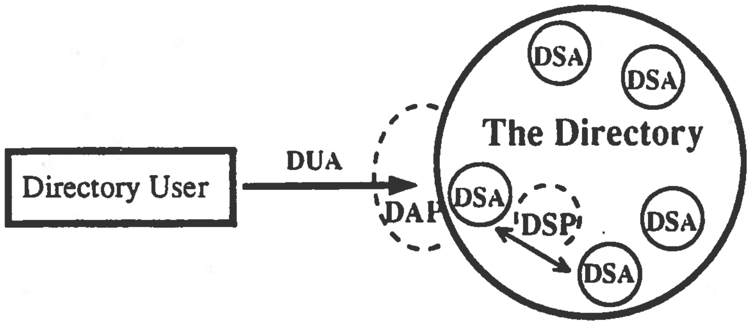
1.1. - What is X.500?

The world of communication is very changed in the last years: today most of academics and researchers people uses computers, gets information through computers, contacts other people through computers and so on. One of the most important problem is how to reach people, databases, archives.

The joined efforts of ISO and CCITT produced in 1988 the Standard 9594 (ISO)[1] and the Recommendation X.500 [2], also known as "The Directory"[3, 4], a global and widely distributed database, providing information on objects belonging to the communication world.

1.2. - X.500: its structure

The information stored in the Directory is known as the Directory Information Base (DIB). It appears as a whole, even if it's distributed in many Directory System Agent (DSA) over the world. The interfaces that people use to interact with the Directory are called Directory User Agent (DUA).



DSA= Directory System Agent, the repository of information
DUA=Directory User Agent, the interface between the user and the Directory
DAP= Directory Access Protocol, which performs the communication between a DUA and a DSA
DSP= Directory System Protocol, which performs the communication between two DSAs

fig . 1

The Directory Information Base consists of entries, describing single *objects*. Each object belongs to a *class*, that defines the set of the object itself. An attribute is made up by a *type* (for instance "telephone number") and the corresponding *value* (+39 51 609822).

The structure of the Directory is a tree and each node is identified by a name, called *Relative Distinguished Name* (RDN). The RDN corresponds to the name of the object on the layer where it is registered. An object is univocally identified by the concatenation of all the RDN from the root to the object itself; the obtained string is called the *Distinguished Name* (DN) of the object.

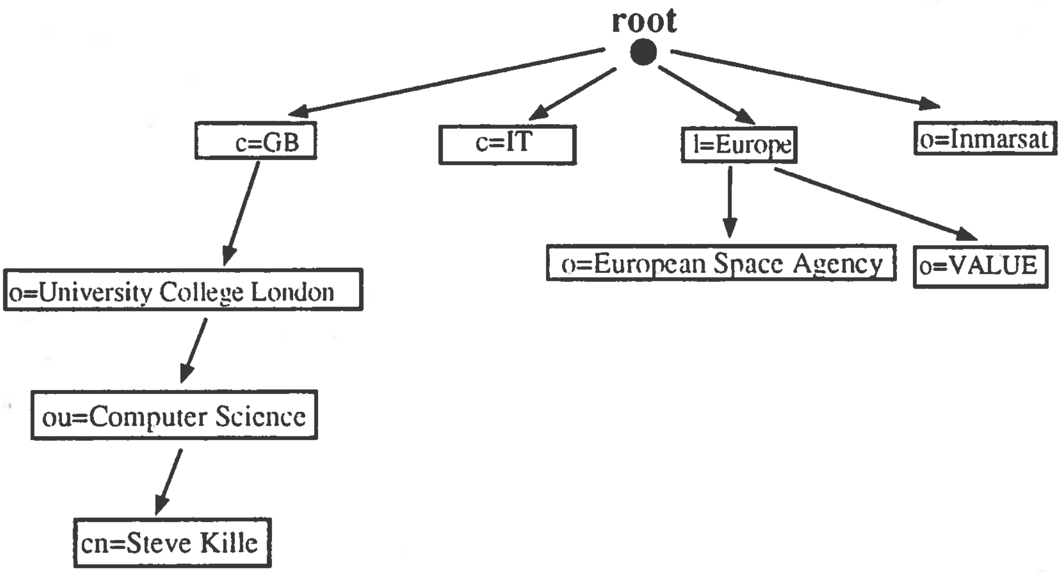


fig . 2

For example, the RDN of Steve Kille is

cn=Steve Kille

while his distinguished name is :

c=GB@o=University College London@ou=Computer Science@cn=Steve Kille

Since the goal of naming is to be "user friendly", a more simple and guessable syntax has also been defined [5] for DN. An example of an User Friendly Name (UFN) is the following:

Steve Kille, Computer Science, University College London, GB

To simplify the query, it is better to use full names instead of acronyms (e.g. University College London instead of UCL). Besides, the more one entry has a short distinguished name (i.e. it is closer to the root), the more it will be easier to find it. Naming policy should be defined according with ISO Standard [6].

1.3. - X.500 in the world

Since 1988, when the International Standard ISO/CCITT was defined, a lot of pilot projects have been developed in all the world to realize "The Directory". The first one was the White Pages Pilot Project, developed in U.S. by NYSERnet to meet the needs of Internet. In Europe the COSINE PARADISE (Piloting A ReseArchers DIrectory Service in Europe) project cordinated the different pilots, providing a central service and developing guidelines. Since 1991 the project holds the root of the world at the University College London.

PARADISE terminated in 1992; the CEC's VALUE project inherited the international coordination. In 1993 the Directory consisted of more than 1 million of entries, stored in about 500 DSAs in the world.

In Italy, after the development of DirWiz by System Wizard within the ESPRIT/THORN Project, CNUCE, Institute of CNR, runs the master DSA for Italy since 1992. In January 1994 the project DIR-ITA started to coordinate the deployment of X.500 within Italy.

1.4. - X.500 in HEP

The High Energy Physics community is heavily present in the Directory: information about people beloging to the most important laboratories and organizations are here stored. A non exhaustive list includes, for example:

Rutherford Appleton Laboratory (RAL)
Stanford Linear Accelerator Center (SLAC)
Deutsches Elektronensynchrotron (DESY)
Argonne National Laboratory
Lawrence Livermore National Laboratory
Lawrence Berkeley Laboratory
Energy Science Network (ESnet)
Brookhaven National Laboratory
Fermi National Accelerator Laboratory

2. - X.500 IN I.N.F.N.

In 1993 INFN started to be concerned with X.500. A new branch of the DIT has been created containing information about the Institute.

The structure of INFN branch is represented in fig. 3.

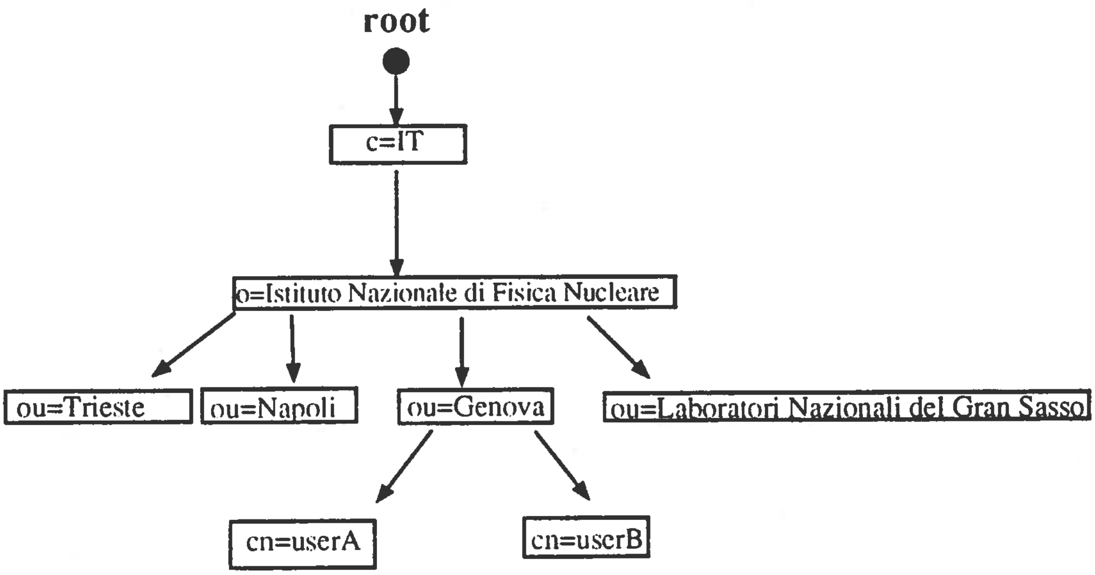

root
c=IT
o=Istituto Nazionale di Fisica Nucleare
ou=Trieste
ou=Napoli
ou=Genova
ou=Laboratori Nazionali del Gran Sasso
cn=userA
cn=userB

fig . 3

Naming structure is consistent with the one already in use in INFN for Internet DNS, DECnet/OSI DNS and with the X.400 address schema.

Under the Organization entry there are the 33 Organizational Units, split up in 19 divisions, 4 national Laboratories, 1 national networking Center, President's office, the central administration and 7 joined groups. Persons are located under each OU. Among them there are also entries for: the Director, the Secretary, the Administrative Secretary, the Postmaster and the Directory Manager, as suggested in the Internet Draft "X.500 Naming Guidelines" [7]. We defined a new object class *ad hoc* for INFN, containing all and only the attributes relevant for our organization. All INFN persons belong to this new class (see appendix A).

A person has a single entry and possibly a set of aliases, each of them containing only essential information to reach the person in that site and a pointer to the main entry for all the orher information. This is useful for people working in more than one Organizational Unit and it avoids duplication of information.

A relevant issue is the inheritance of attributes: since many information concerning a person often are the same of the Organizational Unit, we defined a set of attribute that, if not explicitly stated, are inherited by a person from its Organizational Unit. These are: locality, province, Organizational Unit name, postal address, telephone number, fax number and the access control list.

2.1. - Implementation

Among the existing implementation [8], we choosed QUIPU, the most widespread one, because it was public domain and it was well tested. It runs over the ISODE (ISO Development Environment) stack distributed by ISODE Consortium and uses TCP/IP as network protocol.

The Directory Server Agent (DSA) to hold the part of the DIT for the organisation "c=IT@o=Istituto Nazionale di Fisica Nucleare" has been installed on a Sun SPARCstation 10.

It is a QUIPU convention that DSAs should be named after endangered south american wildlife [9]. Choosing between the suggested names, we called our server "Arapaima". Since it's the master DSA for a national organization, it's immediately under the root for c=IT.

Since at present a single server contains the information for the whole organisation, to provide fault tolerance we established peer to peer agreements with managers of other DSAs: each of them holds slave copies of other's entries. Slave entries refresh is provided via the Directory Server Protocol (DSP) (see fig. 1), that is the protocol used between DSAs to communicate.

As the usage of the service will increase, other DSAs will be installed within INFN, to act as slaves and also to act as masters for part of the organisation. This decentralization will be completely transparent for end users.

The Directory User Agents (DUAs) can access the DSA via the Directory Access Protocol (DAP). DAP is an OSI protocol and requires at least the upper layers of the OSI stack (i.e. a full OSI stack or the ISODE stack). Thus, a DAP-based DUA can't be easily installed on every machine. For this reason we also configured an LDAP (Lightweight Directory Access Protocol)[10] server, that provides communications between DSA and DUA using TCP/IP.

2.2. - Management and security

Since INFN hold its information in a single server, the management is completely centralized. Data collected in the whole Istitute have been initially inserted from the staff at CNAF. To guarantee a useful and reliable service, it's necessary that the information is always kept up to date. Because of the large amount of data, the best solution is a distributed upgrade of them, as described below.

A central DSA manager act as a reference point outside of INFN and coordinates the service inside the organization; in each division, the local X.500 manager adds and removes entries of people belonging to his division and he's responsible to not distribute reserved information. He also supply each user with a password. Each person, through a user friendly DUA, has to keep up to date his own entry.

Security is guaranteed through Access Control Lists (ACL) and passwords.

2.3. - User Interfaces

There are two main classes of Directory User Agents: for management and for simple query.

Here is a list of DUAs and other access tools available to query and/or browse the X.500 service.

WTEL. This is a very simple interface available for VAX/VMS as well for Unix systems, developed at INFN - CNAF. The VMS version needs a WWW client (such as Lynx), while the Unix version uses LDAP. WTEL is installed on almost all the machines of INFN. Just type:

```
wtel "name surname"
```

to only search people in the INFN branch of the DIT.

GO500GW Access trough a gateway between gopher and X.500. Using a gopher client you can connect to the URL (Unique Resource Locator):

```
gopher://x500.infn.it:7777/
```

and then navigate the X.500 tree, starting from the root of the world. It has been developed at the University of Michigan.

WEB500-GW Access through a gateway between WWW (World Wide Web) and X.500. Using a WWW client and connecting to the URL

http://x500.infn.it:8888/

you can browse the whole tree. The starting point is INFN root. This gateway is more sofisticated and complete than the previous one, since it permits to retrieve more information. This tool has been developed at the Technical University Chemnitz, Germany.

X500FIND Access through a gateway between WWW (World Wide Web) and X.500. This gateway has been developed at INFN - CNAF and search for people inside INFN. To query about a person, use a WWW client (e.g. Mosaic, Lynx...) to reach:

http://www.infn.it/cgi-bin/x500find

Otherwise, you can reach

http://www.infn.it/

then select "Phonebooks" and "INFN Phonebook".

Using a WWW client you can also reach the gopher to X.500 gate way described above:

http://www.infn.it/pub/PhoneBooks.html

X500-QUERY This service allows you to query the Directory using Electronic mail. Send a message to the Internet address

x500-query@x500.infn.it

and you will receive detailed informations about how to use the service. To query for a person, for example, the body of the message should contain: "find name surname".

DE (Directory Enquire). Developed by the COSINE Pilot Project, translated in italian by the DIR-ITA Project Staff, it's of simple usage to find information about people. You can reach a public access DE issuing:

```
telnet dsa.nis.garr.it / login: de
```

Next interfaces allow you either to modify the information present in the Directory or simply to query them.

maX.500. This is a user friendly interface based on LDAP and running on Macintosh. Originally developed at the University of Michigan, it has been modified at INFN - CNAF to meet our requirements, and it has also been translated in italian. The latest version is available for anonymous ftp:

ftp://ftp.infn.it/x500/max500_infn_2.0

This version allows you to modify existing entries, but not to add new ones. See Appendix B for an example.

IDM (Interactive Directory Manager). This is the most complete interface among the ones here described. It's intended to be used by the Directory Managers of the Organizational Units of INFN, rather than by normal users. It's a powerful interface that allows any kind of operation. It has been developed by the COSINE Pilot Project, translated in italian by DIR-ITA and modified at INFN - CNAF to meet INFN needs. It uses DAP to talk to the Directory, and can be reached via:

telnet x500.infn.it / login: idm

3. - FUTURE TRENDS

At present, X.500 in the world is mainly used to provide a global "White Pages" service and also INFN acted in this direction.

In reality, the capabilities offered by the Directory Service are quite larger and a few experiments have been carried out.

S. Kille in [11] proposed an experimental new mechanism to access and manage domain information on the Internet, mapping domains onto X.500.

The proposal above has been recently implemented at the University of Minho (Portugal), by developing some tools to dinamically load DNS information into X.500 [12].

U. Eppenberger in [13] examines the X.500 Directory Service usage for X.400 e-mail concerning naming, addressing and routing.

Recently, Brunel University in UK developed a project called ABDUX (Accessing Bibliographic Data Using X.500).

An interesting task will be to study the interworking between X.500 tools (servers and clients) using TCP/IP and other using CLNS as network protocol.

A survey of advanced usages of X.500 is described in [14].

4. - CONCLUSIONS

The task of creating a White Pages service in INFN can be considered complete: more then 1800 entries of persons have been stored in the Directory and can be queried from all the world. At present, our logs show nearly 3000 queries per week and we expect this number will increase as soon as this service became more popular.

In the future studies will be undertaken on how to use the Directory as support for network services in INFNet (the INFN network).

Acknowledgment

Many persons in INFN cooperated in X.500 development: firstly, all the staff at CNAF, and particularly Attilio Castelvetri for his help in data processing, Antonia Ghiselli for the useful suggestions and Davide Salomoni for the help in writing X500FIND.

BIBLIOGRAPHY

[1] CCITT Blue Book. *Data Communication Network - Directory -Recommendations X.500-X.521*. ITU-International Telecommunication Union, Dec. 1988

[2] ISO/IEC International Organization for Standardization and International Electrotechnical Committee. *Open Systems Interconnection - The Directory - International Standard 9594-1*, Dec. 1988.

[3] C.Weider et al., *Technical Overview of Directory Services Using the X.500 Protocol*, RFC 1309, March 1992

[4] C. Weider & J. Reynolds, *Executive Introduction to Directory Services Using the X.500 Protocol*, RFC 1308, March 1992.

[5] S. Kille, *Using the OSI Directory to achieve User Friendly Naming*, RFC 1484, July 1993.

[6] ISO/IEC International Organization for Standardization and International Electrotechnical Committee. *Open Systems Interconnection* - Procedures for the operation of OSI Registration Authorities: General Procedures - *International Standard 9834-1*, Apr. 1993.

[7] P. Barker et al., *Naming and Structuring Guidelines for X.500 Directory Pilots*, Internet-Draft, Dec. 1993.

[8] A. Getchell & S. Sataluri, *A Revised catalog of available X.500 Implementations*, Internet-Draft, Oct. 1993.

[9] ISODE Consortium Limited, *Administrator's Guide - Directory services*, vol. 5, London 1993.

[10] W.Yeong et al., *Lightweight Directory Access Protocol*, RFC 1487, July 1993.

[11] S.Kille, *X.500 and domains*, RFC 1279, Nov. 1991.

[12] Costa A. et al., *Accessing and managing DNS information in the X.500 Directory*, Proceeding of the 4th Joint Networking Conference, Throndheim, NO, May 1993.

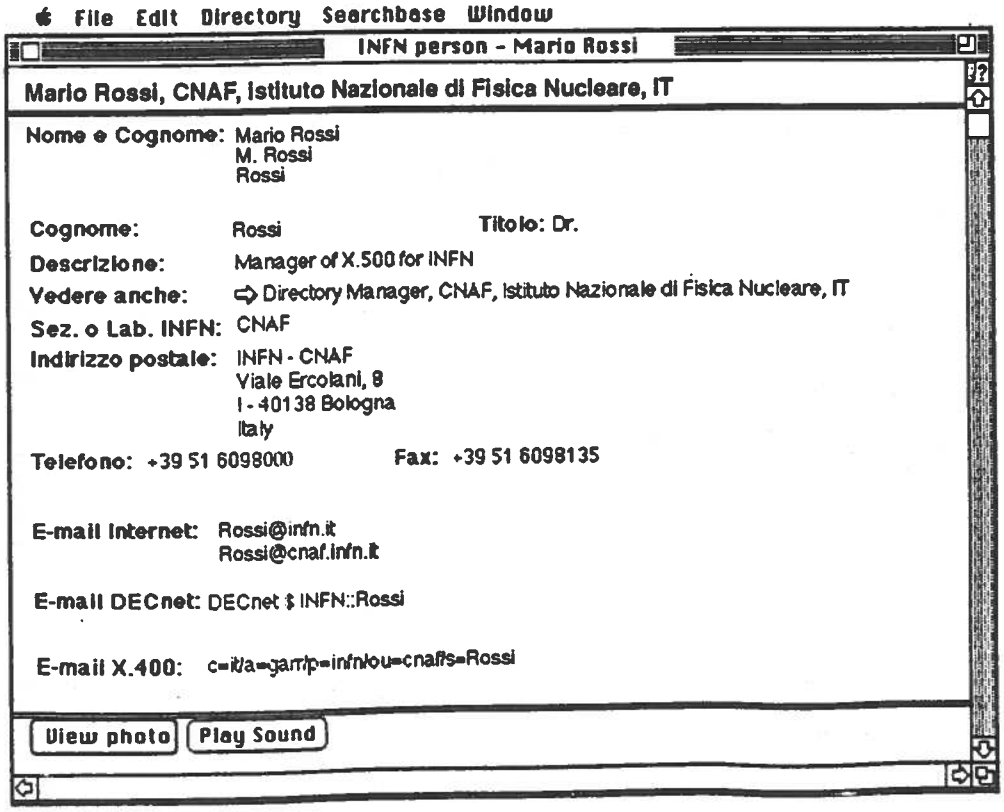
[13] U. Eppenberger, *X.500 directory service usage for X.400 e-mail*, Computer Networks for Research in Europe n. 1: Computer Networks and ISDN Systems 25, Suppl. 1 (1993) S3-8; September 1993.

[14] C.Weider & R. Wright, *A survey of advanced Usages of X.500*, RFC 1491, July 1993.

Appendix A: form for INFN people

```
commonName=
surname=
personalTitle=
description=
OrganizationalUnitName=
roleOccupant=
seeAlso=
userPassword=
userId=
postalAddress=
postOfficeBox=
localityName=
stateOrProvinceName=
telephoneNumber=
facsimiletelephoneNumber=
mobileTelephoneNumber=
telexNumber=
X121Address=
textEncodedORaddress=
rfc822Mailbox=
othermailBox=
favouriteDrink=
objectclass=perINFN & person & organizationalPerson & newPilotPerson
```

Appendix B: screendump of MaX.500 modified for INFN



Mario Rossi, CNAF, Istituto Nazionale di Fisica Nucleare, IT

Nome e Cognome: Mario Rossi
M. Rossi
Rossi

Cognome: Rossi **Titolo:** Dr.

Descrizione: Manager of X.500 for INFN

Vedere anche: ⇨ Directory Manager, CNAF, Istituto Nazionale di Fisica Nucleare, IT

Sez. o Lab. INFN: CNAF

Indirizzo postale: INFN - CNAF
Viale Ercolani, 8
I - 40138 Bologna
Italy

Telefono: +39 51 6098000 **Fax:** +39 51 6098135

E-mail Internet: Rossi@infn.it
Rossi@cnaf.infn.it

E-mail DECnet: DECnet $ INFN::Rossi

E-mail X.400: c=it/a=garr/p=infn/ou=cnaf/s=Rossi