Network Working Group
INTERNET–DRAFT

S.E. Kille
University College London
February 1991

Overall plan of the IETF Working Group on OSI Directories (OSI-DS) to build an Internet Directory using X.500

Status of this Memo

The IETF has established a Working Group on OSI Directory Services (IETF-OSI-DS). A major component of the initial work of this group is to establish a technical framework for establishing a Directory Service on the Internet, making use of the X.500 protocols and services [CCI88b]. This document summarises the plan established by the working group to achieve this, and describes a number of RFCs which the working group will write in order to establish the technical framework.

This draft document will be submitted to the RFC editor as an informational document. Distribution of this memo is unlimited. Please send comments to the author or to the discussion group <osi-ds@CS.UCL.AC.UK>.

1 Introduction

There is substantial interest in establishing an OSI Directory Service on the Internet. There is pressure to establish a number of services on the Internet, including:

- White Pages lookup of users.
- Support for OSI Applications.
- Support for X.509 Authentication for a range of application, including Privacy Enhanced Mail [Lin89].

The OSI Directory is viewed as the best basis for achieving these services, for both technical and political reasons.

The OSI Directory Standards do not contain sufficient information to enable such a service to be built. Full openness and interoperability are a key goal, so service must not depend on private extensions or informal agreements. This document describes the missing components, and suggests a plan for filling in the holes.

The activity is being limited to (reasonably well) understood issues. This means that whilst we will attempt to solve a wide range of problems, that not all (potential) requirements will necessarily be met.

This activity is being done in conjuction with RARE WG3 directory subgroup. The IETF WG and the RARE WG have a common technical mailing list. It is intended that this will lead to a common European and North American approach.

2 Schema

A Directory needs to be used in the context of an Information Framework. The standard directory provides a number of a attributes and object classes to enable basic operation. It is certain that the Internet Community will have requirements for additional attributes and object classes. There is a need to establish a mechanism to register such information.

Pilots in the European RARE Community and the US PSI White Pages Pilot have based their information framework on the THORN and RARE Naming Architecture [Kil89]. It is proposed to use this architecture for the Internet Pilot, in conjunction with COSINE based piloting in Europe. A revised version of the Naming Architecture will be produced, with a mechanism for registration of new attributes and object classes will be developed into an RFC.

3 Use on the Internet

It is a recognised policy on the Internet to deploy OSI Applications over non-OSI lower layers (such as RFC 1006). This policy allows deployment of OSI Applications before an OSI lower layer infrastructure has been deployed. Thus, an Internet Pilot will decouple deployment of the OSI Directory from deployment of the OSI lower layers. An pilot will not make any mandatory requirements about use of lower layers. When configuring the pilot, variations in the lower layers must be considered. The following options are possible:

- Use of OSI Network Service (Connection Oriented or Connectionless). It is seen as fundamental to allow use of the OSI lower layers.
- Operation over TCP/IP using RFC 1006 [RC87]. This is a practical requirement of deployment at very many Internet sites, and is the basis of the existing pilot.
- X.25(80) will probably not be used in the core infrastructure of the Internet Directory Pilot, but is the basis of some European activities. It may be needed later to interconnect with US commerical systems not on the Internet. There will be a practical need to interwork with DSAs which only support this stack.

This approach has the following implications.

1. There is a need to represent TCP/IP addresses within OSI Network Addresses. An RFC will be developed.
2. It will be desirable to have a uniform method to present Network Addresses of this style. Therefore a string representation should be developed into an RFC.
3. This choice leads to the situation where not all DSAs can communicate directly due the different choice of lower layers. This is already a practical result of many European sites operating DSAs over X.25. There may be a requirement to extend the distributed operations, so that there is no requirement for full connectivity. This problem should be handled in the RFC developed to deal with replication issues.
4. When the pilot is deployed, the issue of which DSAs operate which stacks must be considered in order to achieve a coherent service.

4 Replication of Knowledge and Data

There are a number of requirements on replication, both of data and knowledge information, which must be met before an Internet Directory can be deployed. The 1988 standard cannot be used as is. Three solutions are noted:

- Wait until the 1992 standard is available
- Attempt to intercept the 1992 standard, probably by specification of subset functionality based on the current working documents, and in particular the CD on replication [CCI90].
- Use an interim approach

It is necessary to define the minimum requirements, and an RFC should be written to specify these.

The third approach will be taken initially. It will be clearly emphasised that this is an interim approach, which will be phased out as soon as the appropriate standards are available and stable. An interim approach, based on the approach used in the QUIPU Implementation and deployed in existing pilots will be used [Kil88]. This will lead to an RFC.

5 Security

A Directory and Security are closely related. There is no requirement for specification of any Internet specific approaches at this stage. Deployment of a directory could be based on one of:

- Read only system, containing only public data and using local modification.
- Use of X.509 authentication, and private access control mechanisms (this will not allow open access control management, but this is not seen as a fundamental problem) [CCI88a].

A RFC on security for the Internet Directory should be developed. This should specify:

- Internet requirements for security in the Directory
- A recommendation of how to use X.509
- Recommendation on service requirements for access control, as a hint to implementors who attempt to intercept the 1992 standard or develop private mechanisms
- A note on security issues (authentication, policy, access control) not being addressed by the standards work, which might require future work
- Requirements and recommendations for implementors (e.g., in terms of maintaining data confidentiality within an Organisation)

6 Presentation of Directory Names

The standard does not specify a means to present directory names to the user. This is seen as a serious deficiency, and a standard for presenting directory names should be developed. The "User Friendly Name" specification by Kille should be developed into an RFC [Kil90].

7 Name Allocation

When the directory is deployed, there will be a need to allocate the top levels of the DIT. Most aspects will need to be tackled on a national basis. This group will consider name allocations at the top of the DIT, and will look at handling of the US part of the DIT. The major aim here will be to ensure that the Internet takes an, approach aligned to that of the NADF (North American Directory Forum).

8 DSA Naming and MD Structure

There are some critical issues related to naming of DSAs and the structure of Directory Management Domains. It is likely that there will need to be an RFC on this area.

9 Relation to DNS

It is important to establish the relationship between the proposed Internet Directory, and the existing Domain Name System. An RFC should be developed on this area.

10 Documents and Timescales

There will be an overall strategy document for deployment of OSI Directories on the Internet. The WG will have a role in production of this document, but its scope will be broader than the WG.

The following work should lead to a set of RFCs. The latest versions can be obtained from the working draft directories of the IETF OSI-DS WG.

Schema

This specifies attributes and object classes for using the directory on the Internet, as described in Section 2.

Network Address Encoding

This describes a means of encoding RFC 1006 addresses within Network Addresses to support the Directory's use of RFC 1006 as described in Section 3.

Address String Encoding

This describes a string representation of OSI Presentation Addresses. The need is noted in Section 3.

Replication Requirements

A statement of Internet Requirements on replication, as described in Section 4.

Replication Solution

The proposed interim Internet approach to replication, as described in Section 4.

Security

A summary of Internet security requirements on the directory as a part of the early deployment.

Directory Name Presentation

A format for presenting directory names to users, and a means of resolving ambiguous names, as described in Section 6.

Relation to DNS (Domains and X.500)

A model relating the DNS and the OSI Directory, as a basis for experimentation on the Internet, as described in Section 9.

References

[CCI88a] The directory — authentication framework, December 1988. CCITT Recommendation X.509.

[CCI88b] The directory - overview of concepts, models and services, December 1988. CCITT X.500 Series Recommendations.

[CCI90] The directory — part 9 — replication, October 1990. ISO/IEC CD 9594-9 Ottowa ouput.

[Kil88] S.E. Kille. The QUIPU directory service. In *IFIP WG 6.5 Conference on Message Handling Systems and Distributed Applications*, pages 173–186. North Holland Publishing, October 1988.

[Kil89] S.E. Kille. The THORN and RARE naming architecture. Technical report, Department of Computer Science, University College London, June 1989. THORN Report UCL-64 (version 2).

[Kil90] S.E. Kille. Using the osi directory to achieve user friendly naming. Research Note RN/90/29, Department of Computer Science, University College London, February 1990.

[Lin89] J. Linn. Privacy Enhancement for Internet Electronic Mail: Part 1 — Message Encipherment and Authentication Procedures. Request for Comments 1113, DDN Network Information Center, SRI International, August 1989.

[RC87] Marshall T. Rose and Dwight E. Cass. ISO Transport Services on top of the TCP. Request for Comments 1006, DDN Network Information Center, SRI International, May 1987.

11 Security Considerations

Security considerations are discussed in Section 5 of this INTERNET–DRAFT .

12 Author's Address

Steve Kille
Department of Computer Science
University College London
Gower Street
WC1E 6BT
England

Phone: +44-71-380-7294

EMail: S.Kille@CS.UCL.AC.UK