Network Working Group
INTERNET–DRAFT *nnnn*

S.E. Kille
University College London
November 1990

Building 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 strategy established by the working group, and describes a number of RFCs which will be written 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>`.

Contents

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 interoperabulty are a key goal, so service must not depend on private extensions or informal agreements. This document describes the missing components, and suggests a strategy for filling in the holes.

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 [Kil89c]. 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 mechansism for registration of new attributes and object classes.

3 Use on the Internet

It is desirable to decouple deployment of the OSI Directory from deployment of the OSI lower layers. For this reason, it is recommended to operate the directory over TCP/IP using RFC 1006 [RC87] in addition to operation over OSI Network Service. This has the following implications:

1. There is a need to represent TCP/IP addresses within OSI Network Addresses. An Internet Draft, based on a paper by Kille, should be taken as a starting point for this [Kil89a]. It will be necessary to have in Internet Standard on this area.
2. It will be desirable to have a uniform method to present Network Addresses of this style. Therefore a string representation should be developed in parallel. The Internet Draft, based on a paper by Kille, should be used as a basis for this [Kil89b].
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 is a requirement to extend the distributed operations, so that there is no requirement for full connectivity. This issue will be dealt with in the documents to be generated according to Section 4.

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. It is clear that the standard cannot be used as is. Three solutions were 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
- Use an interim approach

It is necessary to define the minimum requirements. An Internet Draft on this will be produced.

Kille believes that all of the key problems have been solved by the QUIPU implementation, in a manner much simpler than that being developed by ISO and CCITT [Kil88]. The existing pilots are a reasonable demonstration of this belief. These mechanisms will be documented, and may be considered as the basis for an Internet approach to replication.

Specifications of alternate interim approaches, especially approaches which intercept the emerging standardisation work, are strongly solicited.

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 specification 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 submitted as an Internet Draft, as a starting point for this work [Kil90].

7 Relation to DNS

It is important to establish the relationship between the proposed Internet Directory, and the existing Domain Name System. One input to this work should be the Internet Draft by Kille, to be updated before the meeting [Kil89d].

8 Documents to be produced

The following Internet Drafts will be produced, to be discussed at the Boulder IETF Meeting.

Schema Cosine and Internet Naming Architecture. P. Barker/S.E. Kille.

Network Address Encoding Revise the Internet Draft [Kil89a]. S.E. Kille.

Address String Encoding Revise the Internet Draft [Kil89b]. S.E. Kille.

Replication Requirements S.E. Kille.

Replication Solution S.E. Kille.

Security P. Yee/B. Manning

Directory Name Presentation Kille

Relation to DNS Kille

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.

[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.

[Kil89a] S.E. Kille. An interim approach to use of network addresses. Research Note RN/89/13, Department of Computer Science, University College London, February 1989. Internet Draft: DRAFT-UCL-KILLE-NETWORKADDRESSES-00.PS.1.

[Kil89b] S.E. Kille. A string encoding of presentation address. Research Note RN/89/14, Department of Computer Science, University College London, February 1989. Internet Draft: DRAFT-UCL-KILLE-PRESENTATIONADDRESSES-00.PS.1.

[Kil89c] 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).

[Kil89d] S.E. Kille. X.500 and domains. Research Note RN/89/47, Department of Computer Science, University College London, May 1989. Also Internet Draft: DRAFT-UCL-KILLE-X500DOMAINS-00.PS.

[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.

9 Security Considerations

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

10 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