

A String Representation of Distinguished Names (OSI-DS 23 (v5))

Status of this Memo

This RFC specifies an IAB standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "IAB Official Protocol Standards" for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Abstract

The OSI Directory uses distinguished names as the primary keys to entries in the directory. Distinguished Names are encoded in ASN.1. When a distinguished name is communicated between to users not using a directory protocol (e.g., in a mail message), there is a need to have a user-oriented string representation of distinguished name. This specification defines a string format for representing names, which is designed to give a clean representation of commonly used names, whilst being able to represent any distinguished name. Please send comments to the author or to the discussion group <osi-ds@CS.UCL.AC.UK>.

Table of Contents

| | |
|---|---|
| 1. Why a notation is needed..... | 1 |
| 2. A notation for Distinguished Name..... | 2 |
| 2.1 Goals..... | 2 |
| 2.2 Informal definition..... | 2 |
| 2.3 Formal definition..... | 3 |
| 3. Examples..... | 6 |
| 4. References..... | 6 |
| 5. Security Considerations..... | 6 |
| 6. Author's Address..... | 7 |

1. Why a notation is needed

Many OSI Applications make use of Distinguished Names (DN) as defined in the OSI Directory, commonly known as X.500 [CCI88]. This specification assumes familiarity with X.500, and the concept of Distinguished Name. It is important to have a common format to be able to unambiguously represent a distinguished name. This might be done to represent a directory name on a business card or in an email

message. There is a need for a format to support human to human communication, which must be string based (not ASN.1) and user oriented. This notation is targeted towards a general user oriented system, and in particular to represent the names of humans. Other syntaxes may be more appropriate for other uses of the directory. For example, the OSF Syntax may be more appropriate for some system oriented uses. (The OSF Syntax uses "/" as a separator, and forms names in a manner intended to resemble UNIX filenames).

2. A notation for Distinguished Name

2.1 Goals

The following goals are laid out:

- o To provide an unambiguous representation of a distinguished name
- o To be an intuitive format for the majority of names
- o To be fully general, and able to represent any distinguished name
- o To be amenable to a number of different layouts to achieve an attractive representation.
- o To give a clear representation of the contents of the distinguished name

2.2 Informal definition

This notation is designed to be convenient for common forms of name. Some examples are given. The author's directory distinguished name would be written:

CN=Steve Hardcastle-Kille, OU=Computer Science, O=University College London, C=GB

This may be folded, perhaps to display in multi-column format. For example:

CN=Steve Hardcastle-Kille,
OU=Computer Science,
O=University College London,
C=GB

Another name might be:

CN=Christian Huitema, O=INRIA, C=FR

Semicolon (";") may be used as an alternate separator.

CN=Christian Huitema; O=INRIA; C=FR

In running text, this would be written as <CN=Christian Huitema; O=INRIA; C=FR>. Another example, shows how different attribute types are handled:

CN=James Hacker,
L=Basingstoke,
O=Widget Inc,
CN=GB

Here is an example of a multi-valued Relative Distinguished Name, where the namespace is flat within an organisation, and department is used to disambiguate certain names:

OU=Sales + CN=J. Smith, O=Widget Inc., C=US

The final example shows quoting of a comma in an Organisation name:

CN=L. Eagle, O="Sue, Grabbit and Runn", C=GB

2.3 Formal definition

A formal definition can now be given. The structure is specified in a BNF grammar in Figure 1. This BNF uses the grammar defined in RFC 822, with the terminals enclosed in <> [Cro82]. This definition is in an abstract character set, and so may be written in any character set supporting the explicitly defined special characters. The quoting mechanism is used for the following cases:

- o Strings containing ",", "+", "=", "<" or ">", "<CR>", "<", ">", "#", or ";".
- o Strings with leading or trailing spaces
- o Strings containing consecutive spaces

There is an escape mechanism from the normal user oriented form, so that this syntax may be used to print any valid distinguished name. This is ugly. It is expected to be used only in pathological cases. There are two parts to this mechanism:

1. Attributes types are represented in a (big-endian) dotted notation. (e.g., 0ID.2.6.53).
2. Attribute values are represented in hexadecimal (e.g., #0A56CF).

The keyword specification is optional in the BNF, but mandatory for this specification. This is so that the same BNF may be used for the related specification on User Friendly Naming [HK93]. When this specification is followed, the attribute type keywords must always be present. A list of valid keywords for well known attribute types used in naming is given in Table 1. This is a list of keywords which must be supported. These are chosen because they appear in common forms of name, and can do so in a place which does not correspond to the default schema used. A register of valid keywords is maintained by the IANA.

Only string type attributes are considered, but other attribute syntaxes could be supported locally. It is assumed that the interface will translate from the supplied string into PrintableString or T.61.

The "+" notation is used to specify multi-component RDNs. In this case, the types for attributes in the RDN must be explicit. The name is presented/input in a little-endian order (most significant component last).

When an address is written in a context where there is a need to delimit the entire address (e.g., in free text), it is recommended that the delimiters <> are used. The terminator > is a special in the notation to facilitate this delimitation.

```

<name> ::= <name-component> ( <spaced-separator> )
        | <name-component> <spaced-separator> <name>

<spaced-separator> ::= <optional-space>
                     <separator>
                     <optional-space>

<separator> ::=  "," | ";"

<optional-space> ::= ( <CR> ) *( " " )

<name-component> ::= <attribute>
                    | <attribute> <optional-space> "+"
                      <optional-space> <name-component>

<attribute> ::= <string>
               | <key> <optional-space> "=" <optional-space> <string>

<key> ::= 1*( <keychar> ) | "OID." <oid>
<keychar> ::= letters, numbers, and space

<oid> ::= <digitstring> | <digitstring> "." <oid>
<digitstring> ::= 1*<digit>
<digit> ::= digits 0-9

<string> ::= *( <stringchar> | <pair> )
            | "'" *( <stringchar> | <special> | <pair> ) "'"
            | "#" <hex>

<special> ::=  ", " | "=" | "'" | <CR> | "+" | "<" | ">"
              | "#" | ";"

<pair> ::= "
<stringchar> ::= any char except <special> or "

<hex> ::= 2*<hexchar>
<hexchar> ::= 0-9, a-f, A-F

```

Figure 1: BNF Grammar for Distinguished Name

Key Attribute (X.520 keys)

| | |
|----|------------------------|
| CN | CommonName |
| L | LocalityName |
| ST | StateOrProvinceName |
| O | OrganizationName |
| OU | OrganizationalUnitName |
| C | CountryName |

Table 1: Standardised Keywords

3. Examples

This section gives a few examples of distinguished names written using this notation:

CN=Marshall T. Rose, O=Dover Beach Consulting, L=Santa Clara, ST=California, C=US

CN=FTAM Service, CN=Bells, OU=Computer Science, O=University College London, C=GB

CN=Steve Hardcastle-Kille, OU=Computer Science, O=University College London, C=GB

CN=Steve Hardcastle-Kille, OU=Computer Science, O=University College London, C=GB

4. References

- [CCI88] The Directory --- overview of concepts, models and services, December 1988. CCITT X.500 Series Recommendations.
- [Cro82] D.H. Crocker. Standard of the format of ARPA internet text messages. STD 11, RFC 822, University of Delaware, August 1982.
- [HK93] S.E. Hardcastle-Kille. Using the OSI directory to achieve user friendly naming. RFC 1484, Department of Computer Science, University College London, July 1993.

5. Security Considerations

Security issues are not discussed in this memo.

6. Author's Address

Steve Hardcastle-Kille
ISODE Consortium
P.O. Box 505
London
SW11 1DX
England

Phone: +44-71-223-4062
EMail: S.Kille@ISODE.COM

DN: CN=Steve Hardcastle-Kille,
O=ISODE Consortium, C=GB

UFN: S. Hardcastle-Kille,
ISODE Consortium, GB