The ISO Development Environment: User's Manual

Update Release

Colin J. Robbins Julian P. Onions
X-Tel Services Ltd

June 17, 1992
(Version 8.0)

Contents

[0] This document (version #1.9) was LaTeXset June 17, 1992 with lplain v2.09-10/29/85.

Preface

The software described herein has been developed as a research tool and represents an effort to promote the use of the International Organisation for Standardisation (ISO) interpretation of open systems interconnection (OSI), particularly in the Internet and RARE research communities.

Notice, Disclaimer, and Conditions of Use

The ISODE is openly available but is **NOT** in the public domain. You are allowed and encouraged to take this software and build commercial products. However, as a condition of use, you are required to "hold harmless" all contributors.

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that this notice and the reference to this notice appearing in each software module be retained unaltered, and that the name of any contributors shall not be used in advertising or publicity pertaining to distribution of the software without specific written prior permission. No contributor makes any representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

All contributors disclaim all warranties with regard to this software, including all implied warranties of mechantibility and fitness. In no event shall any contributor be liable for any special, indirect or consequential damages or any damages whatsoever resulting from loss of use, data or profits, whether in action of contract, negligence or other tortuous action, arising out of or in connection with, the use or performance of this software.

As used above, "contributor" includes, but is not limited to:

The MITRE Corporation
The Northrop Corporation
NYSERNet, Inc.
Performance Systems International, Inc.
University College London
The University of Nottingham
X-Tel Services Ltd
The Wollongong Group, Inc.
Marshall T. Rose
Colin J. Robbins
Julian P. Onions

Revision Information

The ISODE-8.0 software is being released as an upgrade to ISODE-7.0. This is the final public release of the ISODE in its current form.

This document is a supplement to the ISODE-7.0 Manual set.

Release Information

This version of ISODE is available from several places:-

- Internet
  If you can FTP to the Internet, you can use anonymous FTP to the host `uu.psi.com [136.161.128.3]` to retrieve `isode-8.tar.Z` in BINARY mode from the `isode/` directory. This file is the *tar* image after being run through the compress program and is approximately 5.5MB in size.

- NIFTP
  If you run NIFTP over the public X.25 or over JANET, and are registered in the NRS at Salford, you can use NIFTP with username "guest" and your own name as password, to access `UK.AC.UCL.CS` to retrieve the file `<SRC>isode-8.tar.Z`. This file is the *tar* image after being run through the compress program and is approximately 5.5MB in size.

- FTAM on the JANET, IXI or PSS
  The source code is available by FTAM at the University College London over X.25 using

  JANET (DTE `00000511160013`)

  IXI (DTE `20433450420113`)

  PSS (DTE `23421920030013`)

  Use TSEL `259` (ASCII encoding). Use the "anon" user-identity and retrieve the file `isode-8.tar.Z` from the `src/` directory. This file is the *tar* image after being run through the compress program and is approximately 5.5MB in size.

  The file service is provided by the FTAM implementation in ISODE 6.0 or later (IS FTAM) and is registered in the pilot OSI Directory below

```
        bells, Computer Science, University College London, GB
```

The ISODE version 7.0 manual is also available from these sites:

- `isode-7-doc.tar.Z`
  This is the LaTeXsource for the entire documentation set. It is a compressed *tar* image (3.5MB).

- `isode-7-ps.tar.Z`
  This contains the five volume manual in PostScript format. It is a compressed *tar* image (4.3MB).

Discussion Groups

The Internet open discussion group `ISODE@NISC.SRI.COM` is used as a forum to discuss ISODE. Contact the Internet mailbox `ISODE-Request@NISC.SRI.COM` to be asked to be added to this list.

Support

Although the ISODE is not "supported" per se, it does have a problem reporting address, `Bug-ISODE@isode.com`. Bug reports relating to the release of ISODE are welcome. Changes will be incorporated into the ISODE Consortium releases (see Appendix E), and not released to the public domain.

Commercial Support

X-Tel Services Ltd provide support for the ISODE and associated packages on an international basis. X-Tel is a founding member of the ISODE Consortium and will continue to provide general assistance and site specific support on a commercial basis. X-Tel will also enhance and market ISODE Consortium product.

Postal address: X-Tel Services Ltd.
University Park,
Nottingham, NG7 2RD
UK

Phone	+44 602 412648
Fax	+44 602 790278
EMail	support@xtel.co.uk

The ISODE CONSORTIUM will maintain a database of companies offering support of the ISODE Package.

Acknowledgements

Since the start of the project, many many people have contributed to the ISODE software. A long list of contributors is given in the ISODE version 7.0 manual. In this section, we include thanks to the people who have contributed to getting *this* version of the software ready.

Paul Barker of University College London. Steve Hardcastle-Kille of ISODE Consortium. Tim Howes of University of Michigan. Mark Mattingley-Scott of IBM Deutschland GmbH. George Michaelson of Univerity of Queensland. Marshall T. Rose of Dover Beach Consultancy Inc. Wengyik Yeong of PSI. Peter Yee of NASA. Alan Young of Concurrent Computer Corporation. The PARADISE project. X-Tel Services Ltd.

cjr & jpo

Nottingham, England
June, 1992

Chapter 1

Introduction

This document contains a set of updates to the version 7 ISODE manual. This document refers to the final public version of ISODE, released as ISODE-8.0. As the changes to the documentation since the 7.0 release have been only minor, it would be wasteful to reproduce the entire manual set.

The following chapters contains a description of the changes to various parts of the ISODE version 7 manual.

Appendix F includes a table of hardware platforms and operating systems this version of ISODE is believed to work on. This information is based upon reports given to us. We do not know how accurate the information is.

Chapter 2

The ISODE Tailoring file

This chapter reflects changes to Chapter 6 of Volume 2 “Tailoring”.

The sub section titled “Bridge X.25” has been removed from Section 6.1.5 “Interface Specific Tailoring”, reflecting the removal of the TP0 bridge from the ISODE.

In the sub section titled “General X.25 Tailoring”, the text for the `x25_dnic_prefix` parameter has been changed to:

> `x25_dnic_prefix` If you use either or both of the preceding two mechanisms [`x25_intl_zero` or `x25_strip_dnic`] then you must use this variable to inform ISODE of the local DNIC for your host.
>
> It can contain more than one DNIC, this is only relevant if `x25_intl_zero` has the value `on`. All DNICs in the list will not have the leading zero added. This is useful for private X.25 networks (such as the european IXI) that do not need leading zeros. Only the first DNIC listed will be used in striping.

Some new sub sections have been added to Section 6.1.5, these are included below.

RTnet-X25/PLUS

X.25 using the Concurrent RTnet-X25/PLUS needs some tailoring as described below. At least one of option must be configured.

`x25_default_line` RTnet-X25/PLUS requires attached lines to be configured with names. This variable determines which named line will be used if an appropriate match is not found in x25_communities (see below).

`x25_communities` pairs of community name and line name to determine which line will be used for a call to a particular community.

TP4

`nsap_default_stack` If the TP4 interface has access to both CONS and CLNS, this parameter is used to determine the default. The value can be either `CONS` or `CLNS`. The default value is `CLNS`. You should also consult *isonsapsnpa*(5), which defines how the default stack can be overridden for specific NSAP addresses.

`local_nsap` A default NSAP address for tsapd to listen on if the `-N` flag is used!

TLI TP4

The following setting are only useful when TP_TLI is defined, that is, the TP4 is provided by the TLI interface.

`tli_cots_dev` The name of the device node used to access COTS (default `/dev/ositpi`).

`tli_clts_dev` The name of the device node used to access CLTS (default `/dev/ositpi`).

ICL TLI TP4

When using TLI on an ICL DRS6000, the following two addressing parameters will need setting:

`tli_initiator_prefix` The subnet name of the network interface to use for outgoing X.25 calls (default `x25_tliin`).

`tli_responder_prefix` The subnet name of the network interface to use for incomming X.25 calls. (default `x25_tlire`).

XTI TP4

The following setting is only useful when XTI is defined. That is TP4 is provided by an XTI interface. XTI is only alpha test in this release.

`xti_tp0_ident` The string value is the string passed to the XTI interface during t_bind for X121 addresses. Default `TOSITP0`.

`xti_tp4_ident` The string value is the string passed to the XTI interface during t_bind for TP4 addresses. Default `TOSITP4`.

Chapter 3

QUIPU

This chapter details changes to the Volume 5 manual: QUIPU.

There have been extensive changes to the Chapter 6: DE. The new chapter is included in its entirety as Appendix A.

There is a new Chapter on "DM tools". These are a set of DISH shell scripts which provide some simple bulk data management functions using DAP.

Chapter 10 has a new sub section on the SearchACL attribute syntax, this is in Appendix C.1.

Chapter 11 of Volume 5 has a new section describing searcl ACLs in more detail. This is included as Appendix D of this document.

It should also be noted that the `QUIPU-support@cs.ucl.ac.uk` support address no longer exists. This has been replaced with a bug reporting address. Any changes required will be incorporated into the ISODE Consortium releases, and not released to the public domain.

```
bug-quipu@isode.com
```

However, it should be noted that the open discussion list

```
quipu@cs.ucl.ac.uk
```

does still exists. Mail

```
quipu-request@cs.ucl.ac.uk
```

to join the discussion.

3.1 Text Changes

The second paragraph of Section 17.2.1, page 201 in volume 5 should read:

> The fields `ca_ext`, `ca_progress`, `ca_requestor` and `ca_aliased_rdns` are provided as they are defined within X.500. Neither the QUIPU DSA or DUA use these fields, but they must be initialized to zero.

The text in Section 17.2.2 "Results" should read:

> The field `cr_aliasdereferenced` is set to `TRUE` if the base object of the operation was an alias, and was dereferenced.
>
> The field `cr_requestor` is the DN of the requestor of the operation. It is only used for secure operations.
>
> The other fields are used by *pepsy* whilst encoding and decoding the structure.

All of the references to *.podrc* in Chapter 9 should be replaced with *.duarc*

Chapter 4

Known Problems

This chapter describes some known problems with the current implementation of ISODE.

Simply Encoded Data

If "user-data" at the presentation layer is simply encoded, ISODE is sometimes unable to decode the data. ISODE always uses fully encoded data. A default context in not proposed by any of the applications, thus simply encoded data is rarely required.

Large RFC-1006 TPDUs

If RFC-1006 is used to transfer a large TPDU, then the current implementation effectively does a read of the RFC-1006 header, followed by `n` bytes of data, as specified in the header.

If `n` is large, it will require several reads to actually read this number of bytes. These reads are done synchronously, one after another until the packet is in. However, if its a large packet and the TCP connection is unreliable, some of the 64K may get dropped and have to be retransmitted. If a router goes down also in this time you can get left hanging. This particularly effects QUIPU.

ACSE Initialisation

During the initialisation stage of an ACSE connection, it is possible for a connect request to momentarily block.

Appendix A

DE

DE (which stands for **D**irectory **E**nquiries) is a directory user interface primarily intended to serve as a public access user interface. It is a successor to, and borrows something of the style of, the *dsc* interface released in a previous version. It is primarily aimed at the novice user, although more sophisticated users should find that it is flexible enough to answer the majority of queries they wish to pose.

DE has more features than those discussed below. However, the program has extensive on-line help as it is envisaged that it will often be used in environments where neither on-line help nor paper documentation will be available.

A.1 Using DE

A.1.1 Starting up

DE will work quite happily without any knowledge of the user's terminal type, assuming a screen size of 80 x 24 in the absence of terminal type information. If, however, the user's terminal type is not recognised by the system, the user will be prompted to try and enter an alternative. The user can examine a list of valid terminal types; typing `<CR>` accepts a terminal type of "dumb".

It is possible to configure DE to force confirmation of screen lengths of greater than 24 lines — this helps with WAN access as some virtual terminal protocols do not propagate the screen size.

A.1.2 Searching for a Person

The interface prompts the user for input with the following four questions:

```
Person's name, q to quit, * to list people, ? for help
:- barker
Dept name, * to list depts, <CR> to search all depts, ? for help
:- cs
Organisation name, <CR> to search 'ucl', * to list orgs, ? for help
:-
Country name, <CR> to search 'gb', * to list countries, ? for help
:-
```

Note from the above example that it is possible to configure the interface so that local values are defaulted: RETURN accepts "ucl" for organisation, and "gb" for country. The above query returns a single result which is displayed thus:

```
United Kingdom
  University College London
    Computer Science
      Paul Barker
        telephoneNumber       +44 71-380-7366
        electronic mail       P.Barker@cs.ucl.ac.uk
        favouriteDrink        guinness
                              16 year old lagavulin
        roomNumber            G21
```

If several results are found for a single query, the user is asked to select one from the entries matched. For example, searching for "jones" in "physics" at "UCL" in "GB" produces the following output:

```
United Kingdom
  University College London

Got the following approximate matches.  Please select one from the
list by typing the number corresponding to the entry you want.

    1 Faculty of Mathematical and Physical Sciences
    2 Medical Physics and Bio-Engineering
    3 Physics and Astronomy
    4 Psychiatry
    5 Psychology
```

Selecting “Physics and Astronomy” by simply typing the number 3, the search continues, and the following is displayed:

```
United Kingdom
  University College London
    Physics and Astronomy

Got the following approximate matches.  Please select one from the
list by typing the number corresponding to the entry you want.

     1 C L Jones     +44 71-380-7139
     2 G O Jones     +44 71-387-7050 x3468  geraint.jones@ucl.ac.uk
     3 P S Jones     +44 71-387-7050 x3483
     4 T W Jones     +44 71-380-7150
```

In this condensed format, telephone and email information is displayed.

A.1.3 Searching for other information

Information for organisations can be found by specifying null entries for the person and department.

Information for departments can be found by specifying null input for the person field.

Information about rooms and roles can be found as well as for people by, for example, entering “secretary” in the person's name field.

A.1.4 Interrupting

If the user wishes to abandon a query or correct the input of a query (maybe the user has mis-typed a name), *control-C* resets the interface so that it is waiting for a fresh query. Typing “q” at prompts other than the person prompt results in the user being asked to confirm if they wish to quit. If the user replys “n”, the interface resets as if *control-C* had been pressed.

A.1.5 Quitting

Type “q” (or optionally “quit” — see below) at the prompt for a person’s name. Type “q” at other prompts, and the user is asked to confirm if they wish to quit. If the use replys “n”, the interface resets to allow a query to be entered afresh.

A.2 Configuration of DE

As DE is intended as a public access dua, it is only configurable on a system-wide basis. DE installs help files and the *detailor* file into a directory called *de/* under `ISODE`’s ETCDIR.

A.2.1 Highly recommended options

The *detailor* file contains a number of tailorable variables, of which the following are highly recommended:

`dsa_address:` This is the address of the access point DSA. If two or more dsa_address lines are given, the first dsa_address is tried first, the second dsa_address is tried if connecting to the first address fails. Third and subsequent dsa_address entries are ignored. If there is no dsa_address entry in the *detailor* file, the first value in the *dsaptailor* file is used.

```
dsa_address:Internet=128.16.6.8+17003
dsa_address:Internet=128.16.6.10+17003
```

`username:` This is the username with which the DUA binds to the Directory. It is not strictly mandatory, but you are strongly encouraged to set this up. It will help you to see who is connecting to the DSA.

```
username:@c=GB@o=X-Tel Services Ltd@cn=Directory Enquiries
```

A.2.2 Variables you will probably want to configure

You will almost certainly want to set at least some of these to suit your local system:

`welcomeMessage:` This is the welcoming banner message. The default is "Welcome to the Directory Service".

```
welcomeMessage:Welcome to DE
```

`byebyeMessage:` This enables/disables the display of a message on exiting DE. This variable takes the values "on" and "off". The message displayed is the contents of the file *debyebye,* which should be placed in the same directory as all DE's help files. The default is not to display an exit message.

```
byebyeMessage:on
```

`default_country:` This is the name of the country to search by default: e.g., "GB".

```
default_country:gb
```

`default_org:` This is the name of the organisation to search by default: e.g., "University College London"

```
default_org:University College London
```

`default_dept:` This is the name of the department (organisational unit) to search by default: e.g., "Computing". This will usually be null for public access duas.

```
default_dept:
```

A.2.3 Attribute tailoring

The following configuration options all concern the display of attributes. The settings in the *detailor* file will probably be OK initially.

`commonatt:` These attributes are displayed whatever type of object is being searched for, be it an organisation, a department, or a person.

```
commonatt:telephoneNumber
commonatt:facsimileTelephoneNumber
```

`orgatt`: These attributes are displayed (as well as the common attributes — see above) if an entry for an organisation is displayed.

```
orgatt:telexNumber
```

`ouatt`: These attributes are displayed (as well as the common attributes — see above) if an entry for an organisational unit (department) is displayed.

```
ouatt:telexNumber
```

`prratt`: These attributes are displayed (as well as the common attributes — see above) if an entry for a person, room or role is displayed.

```
prratt:rfc822Mailbox
prratt:roomNumber
```

`mapattname`: This attribute allows for meaningful attribute names to be displayed to the user. The attribute names in the quipu oidtables may be mapped onto more user-friendly names. This allows for language independence.

```
mapattname:facsimileTelephoneNumber fax
mapattname:rfc822Mailbox electronic mail
```

`mapphone`: This allows for the mapping of international format phone numbers into a local format. It is thus possible to display local phone numbers as extension numbers only and phone numbers in the same country correctly prefixed and without the country code.

```
mapphone:+44 71-380-:
mapphone:+44 71-387- 7050 x:
mapphone:+44 :0
```

`greybook`: In the UK, big-endian domains are used in mail names. By setting this variable on, it is possible to display email addresses in this order rather than the default little-endian order.

```
greyBook:on
```

`country`: This allows for the mapping of the 2 letter ISO country codes (such as GB and FR) onto locally meaningful strings such as, for english speakers, Great Britain and France.

```
country:AU Australia
country:AT Austria
country:BE Belgium
```

A.2.4 Miscellaneous tailoring

There are a number of miscellaneous variables which may be set.

`maxPersons`: If a lot of matches are found, DE will display the matches in a short form, showing email address and telephone number only. Otherwise full entry details are displayed. This variable allows the number of entries which will be displayed in full to be set — the default is 3.

```
maxPersons:2
```

`inverseVideo`: Prompts are by default shown in inverse video. Unset this variable to turn this off.

```
inverseVideo:on
```

`delogfile`: Searches are by default are logged to the file *de.log* in `ISODE`s LOGDIR. They can be directed elsewhere by using this variable.

```
delogfile:/tmp/delogfile
```

`logLevel`: The logging can be turned off. It can also be turned up to give details of which search filters are being successful — this will hopefully allow some tuning of the interface.

- Level 0 — turns the logging off.
- Level 1 (the default level) — logs binds, searches, unbinds
- Level 2 — gives level 1 logs, and logging analysis of which filters have been successful and which failed

```
logLevel:2
```

`remoteAlarmTime:` A remote search is one where the country and organisation name searched for not the same as the defaults. If the search has not completed within a configurable number of seconds, a message is displayed warning the user that all may not be well. The default setting is 30 seconds. The search, however, continues until it returns or is interrupted by the user.

```
remoteAlarmTime:30
```

`localAlarmTime:` As for *remoteAlarmTime*, except for local searches. The default setting is 15 seconds.

```
localAlarmTime:15
```

`quitChars:` The number of characters of the word "quit" which a user must type to exit. The default setting is 1 character.

```
quitChars:1
```

`allowControlCtoQuit:` This enables or disables the feature where a user may exit the program by typing `control-C` at the prompt for a person's name. The default setting is on.

```
allowControlCtoQuit:on
```

`wanAccess:` This enables the feature where a user is asked to confirm that the size of their terminal is really greater than 24 lines. This helps with telnet access if the screen size is not propagated. The default setting is off.

```
wanAccess:on
```

A.3 Dynamic tailoring

It is possible for a user to modify some variables used by DE while running the program. In particular, this allows a user to recover from a situation where the terminal emulation is not working correctly — an apparently frequent occurrence!

Dynamic tailoring of variables is offered by use of the SETTINGS help screen. Typing `?settings` at any prompt will display the current settings of dynamically alterable variables. The user is then offered the opportunity of modifying the variables. Variables which may currently be altered in this way are:

`termtype` The user's terminal type, as set in the UNIX "TERM" environment variable.

`invvideo` Turn inverse video "on" (if the terminal supports it) or "off"

`cols` Set the width of the screen to a number of columns

`lines` Set the length of the screen to a number of lines

Appendix B

DM Tools

DM tools are a set of shell scripts which provide some simple bulk data management functions using DAP. The tools have the following characteristics.

- They obviate such skulduggery as editing EDB files on the DSA machine.
- They provide some ability to add, modify and delete entries and attributes.
- They will play a part in managing data from multiple sources, but there are several limitations (see caveats later).
- They will not handle large numbers of thousands of entries in one go, but have been used with success with a few thousand entries.
- Based on DISH commands with lashings of shell and [gn]awk.

B.1 How the Tools Work

The tools are driven by data in a syntax very similar to the EDB files. A special-purpose difference tool is used to work out differences between the current version of the data and the previous version. Another tool processes the resultant differences (which may, of course, be the original file the first time round) and translates this data into a shell script of the DISH commands required to update the directory appropriately. Run the resultant shell script to apply the modifications.

B.2 The Bulk Data Format — dmformat

This is very similar to the EDB format. The differences are as follows:

EDB	DMFORMAT
DIT hierarchy mapped onto UNIX directory structure	Flat file with embedded info saying where entries should be loaded in the DIT
Files start with: MASTER date in UTC format	File don't start with ... File contains ”rootedAt” info
	Syntax includes mechanism for specifying deletion of an entry / attribute
Can only represent one set of sibling entries	Can represent information in an entire subtree or collection of subtrees

Comments may be interspersed throughout the file. A comment line begins with a “#” character.

rootedAt indicates the parent node in the DIT for subsequent entries in the file. Separate a rootedAt line from entries by one or more blank lines.

A set of entries follows a rootedAt line. These are formatted in the same way as in an EDB file: i.e., an entry is a sequence of attribute type-value pairs, where the first pair is the RDN for the entry.

Entries are separated from other entries by blank lines.

In addition to the conventional syntax it is possible to specify deletion of entries and attributes.

- Specify entry deletion by prefixing the RDN with the “!” character.

- Specify attribute value deletion by prefixing the attribute type=value line with a “!” character.

A file can contain information for many DIT subtrees by including more rootedAt lines.

B.3 dmformat — An Example

```
#subsequent entries are relative to this point
# in the DIT
rootedAt= c=gb@o=UCL@ou=CS

# add this entry with these attributes
#   if it doesn't already exist
# try to add in these attribute values if
#   the entry already exists
cn=Paul Barker
surname=Barker
telephoneNumber=+44 71 380 7366
objectClass=organizationalPerson & quipuObject & ...

# Add the first telephone number attribute
# value and delete the second
cn=Steve Kille
telephoneNumber=+44 71 380 7294
!telephoneNumber=+44 71 380 1234

# Delete this entry
!cn=Colin Robbins
# don't have to supply attributes, but can
# if you like
!telephoneNumber=+44 71 387 7050 x3688

#subsequent entries are relative to this point
# in the DIT
rootedAt= c=gb@o=UCL@ou=Physics
```

B.4 Using the Tools

The tools can be used to load the database initially as follows:

- Produce a file "newfile" of entries to be loaded
- Make a file of DISH operations to effect the update

  ```
  crmods < newfile
  ```
- Apply the updates

  ```
  sh modfile
  ```

It can also be used for subsequent amendments

- Create a file of difference data

  ```
  dmdiff oldfile newfile > difffile
  ```
- Create a shell/DISH script to do the update

  ```
  crmods < difffile
  ```
- Apply the updates

  ```
  sh modfile
  ```

There are examples of using the tools and sample Makefiles in the README file accompanying the software.

B.5 Preparing Data for use with DM Tools

The tools will work more efficiently if the following guidelines are followed:

- Attribute type strings in DM files should be the same as those written out by DISH when using "showentry -edb"

  In practice this means using the abbreviated attribute names as specified in $(ETCDIR)/oidtable.at. E.g., use "cn" rather than "commonName", and "mail" rather than "rfc822Mailbox".

- Be consistent with capitalisation and case in general between DM files produced from the various sources.

- Attribute values with DN syntax should have the country name part represented in capitals, as in "c=GB". This is because QUIPU always writes them out that way. In all other cases, QUIPU maintains the case with which entries' attributes are created.

B.6 Some Specific Shortcomings of the DM Tools

- Scale — the shell script, `modfile,` which crmods produces, is very large for substantial amounts of data or data differences

  It may be more manageable to split data into a set of department files, as for EDBs, and apply set of updates.

- Matching of attribute types and attribute values is case-sensitive, whereas almost always it should be case-independent.

  In practice this is not too much of a problem

  - At worst, it means that too many "differences" are discovered
  - QUIPU does the "right thing" anyway

- No explicit mechanism for renaming entries — achieved by deleting entry with old name and creating a new entry.

  You may thus discard attribute information which has been loaded from another source.

- Tools have no knowledge that entries may be mastered by more than one source.

  If an entry is deleted from one source, it will be deleted from the Directory even if the entry still exists in another source. This may, or may not, be want you want!

- No explicit support for maintenance of seeAlso, roleOccupant and other attributes which have DN syntax.

  All necessary management to avoid “dangling pointers” must be achieved externally

- No support for management of aliases

- Updating over DAP can be rather slow for entries with large numbers of siblings (in QUIPU terms, in a large EDB file).

  There is a solution — use the TURBO_DISK option when compiling QUIPU. This makes use of GNU’s gdbm package. Consider this if you do a lot of updating and you have large EDB files.

- There are some known bugs. Inherited attributes are not always handled correctly, and problems with eDBInfo have been reported.

B.7 General Data Management Problems Not Catered For

- Management of data from multiple sources is very difficult — no support for merging data from different sources, or for consistent deletion.

- No framework for discrimination between quality of data sources — this must be handled manually

- Relying on diffs not really satisfactory — need to rebuild database periodically from source data

- Naming of entries — DM tools offer no help with naming to person maintaining the Directory database. This administrator should be aware of at least the following problems

  - Two sources may name an entity differently

    ```
    source one: P Barker
    source two: Paul Barker
    ```

- Need to be careful that no duplicate RDNs are formed when processing the source data into EDBs or DM files.
  - If building EDBs, QUIPU will detect multiple RDNs as it loads its database.
  - DM tools will perform multiple updates on a single entry
- Even in case where one is loading from a single source, the name which is systematically derivable may be unsatisfactory. E.g.,

  `PHYS & ASTRO`

  rather than

  `Physics and Astronomy`
- A source's vies of what constitutes a department may be parochial, suiting particular requirements. For example, the UCL telephone directory database has the following two departments

  ```
  BIOLOGY (DARWIN)
  BIOLOGY (MEDAWAR)
  ```

  whereas the University view, which must be represented, is that there is just a single "Biology" department
- Need to be careful when joining departments in this way that no RDN clashes occur. If they do occur, a solution is to name entries with multiple value RDN.

  cn=Fred Bloggs%ou=Biology (Medawar)

Appendix C

Attribute Synatxes

The sections in this appendix should be placed at the end of Section 10.3 "COSINE/Internet Attribute Syntaxes" of the Version 7.0 manual.

C.1 SearchACL

QUIPU Attributes
searchACL

```
<searchaclvalue>::= <aclwho> "#" <access> "#" <attrs>
                    "#" <scope>
                    [ "#" <max-results> "#" <partialresults>
                    [ "#" <minkeylen> ]]
<access>        ::= "search" | "nosearch"
<attrs>         ::= "default" | <attr-list>
<attr-list>     ::= <attributetype> | <attributetype>
                    "$" <attr-list>
<scope>         ::= <singlescope> | <singlescope>
                    "$" <scope>
<singlescope>   ::= "subtree" | "singlelevel" | "baseobject"
<max-results>   ::= <integer>
<partialresults>::= "partialresults" | "nopartialresults"
<minkeylen>     ::= <integer>
```

The use of the search ACL attribute is discussed in Section D.

C.2 ListACL

QUIPU Attributes
listACL

```
<listaclvalue>  ::= <aclwho> "#" <access> "#" <scope>
                        [ "#" <max-results> ]
<access>        ::= "list" | "nolist"
<scope>         ::= "entry" | "children"
<max-results>   ::= <integer>
```

The use of the list ACL attribute is discussed in Section D.1.

C.3 AuthPolicy

QUIPU Attributes
authPolicy

```
<authpvalue>    ::= <modpolicy> "#" <readpolicy>
                    "#" <searchpolicy>
<modpolicy>     ::= <authpolicy>
<readpolicy>    ::= <authpolicy>
<searchpolicy>  ::= <authpolicy>
<authpolicy>    ::= "trust" | "simple" | "strong"
```

Appendix D

Search Access Control

The access control described above is sufficient to protect individual entries from unauthorized access, but it does little to protect the directory as a whole from "trawling": the disclosure of large amounts of organizational data or structure information by repeated searches. In the past, the administrative size limit was the only control on such access. The search ACL is designed to allow much more flexible control on the types on searches performed and the number of results that can be obtained by a directory user.

A search ACL belongs to a single entry and specifies restrictions on searches involving that entry and possibly its descendants. A search ACL scope must be specified. A scope of "subtree" means the search ACL applies during subtree searches involving the entry and its descendants. Note that the subtree search must be rooted at or above the entry containing the search ACL for the ACL to apply. A "singlelevel" search ACL applies only during a single level search rooted at the entry containing the ACL. Note that the subtree and single level scopes are disjoint: a subtree search ACL has no bearing on a single level search and vice versa.

A search ACL with scope "baseobject" applies to the entry during any type of search, and can thus be used to provide discretionary access control for searches in a way similar to normal access control.

The simplest and most restrictive application of a search ACL is to prevent searching on certain attribute types. For example, the following search ACL would not allow anyone to perform any type of search by the userPassword attribute in the subtree rooted at the entry containing the search ACL (or in its children).

```
sacl= others # nosearch # userPassword \
           # subtree $ singlelevel
```

The access selector for a search ACL is the same as for a normal QUIPU ACL. Note that a search started at a point in the DIT below the entry containing a search ACL is not constrained by that search ACL.

To allow searches by certain attributes, but to limit the number of results that can be returned, a search ACL like this may be used:

```
sacl= others # search # commonName $ surname \
           # subtree # 10 # partialresults
sacl= others # nosearch # default # subtree
```

This allows others to search only by the attributes commonName and surname, returning at most 10 matches. If "trawling" is a concern, the search ACL above can be modified to not return any results if the size limit specified is exceeded:

```
sacl= others # search # commonName $ surname \
           # subtree # 10 # nopartialresults
sacl= others # nosearch # default # subtree
```

Note that both of the preceeding examples only restrict subtree searches. If single level searches are to be restricted also, the scope should be changed to "subtree $ singlelevel." Note also that the attributes not specified in another search ACL may be referred to by using the "default" keyword. In the example above, this capability is used to disallow searches on any attributes but commonName and surname.

An individual entry may protect itself from being found by certain types of searches by using the "baseobject" search ACL scope. For example,

```
sacl= others # nosearch # commonName $ surname # baseobject
```

Finally, it may be desirable to restrict certain types of searches below an entry. For example, if not checked, an effective dumping technique is to do repeated searches of the form cn=a*, cn=b*, etc. This technique is not entirely thwarted by the "nopartialresults" capability described above, because a clever and determined attacker can construct repeated range filters where the range is small enough not to exceed the size limit.

As a defense against such attacks, a minimum substring key length may be specified in a searchACL. This minimum length is also used as the minumum prefix that must be common to any range queries using the inequality operators. For example, a search acl like this one

```
sacl= others # search # default # subtree # 10 \
           # nopartialresults # 3
```

specifies that others may perform subtree searches by the default attribute set, returning at most 10 matches. No matches will be returned if the limit of 10 is exceeded. Furthermore, any substring queries must contain a substring that is at least 3 characters long, and any inequality range queries must involve values whose first 3 characters are the same. To see how this works, consider the following queries and the reason they are either accepted or rejected because they violate the above search ACL.

Filter	Accepted?	Explanation
cn=a*	no	maximum substring length is 1
cn=aa*	no	maximum substring length is 2
cn=*a*	no	maximum substring length is 1
cn=abc*	yes	maximum substring length is 3
cn=a*abcd*	yes	maximum substring length is 4
(cn>=a & cn<=b)	no	common prefix length is 0
(cn>=aa & cn<=ab)	no	common prefix length is 1 (a)
(cn>=abcdef & cn<=abcghi)	yes	common prefix length is 3 (abc)

D.1 List ACL

Just as a search ACL can be used to control access to groups of entries during search operations, the list ACL can be used to control access during list operations. A list ACL may apply to an individual node, or a node's children. For example, to prevent everyone except those users in the US from listing a particular entry, a user might add the following list ACL to the entry:

```
lacl= others # nolist # entry
lacl= prefix # c=US # list # entry
```

The access selector portion of a list ACL is the same as for a normal QUIPU ACL.

A list ACL can also be used to control the listing of a node's children. In addition to specifying whether a particular user can list the children or not, one can specify the maximum number of children that will be returned by a single list operation. For example, to prevent everyone except US users from listing the children of an entry, that entry should have the following list ACL:

```
lacl= others # nolist # children
lacl= prefix # c=US # list # children
```

A limit on the number of children returned from a list (10 in this example) may be imposed by the following:

```
lacl= others # list # children # 10
```

D.2 Authentication Policy

With discretionary access control, search access control, and list access control, there is a need to authenticate the party requesting access. It should be specifiable on a per entry basis what form this authentication should take for it to be believed. For example, one trusting individual might view no authentication as sufficient, allowing access over unauthenticated DSP links. Another user might be satisfied with simple authentication. Still another security conscious individual might not be satisfied with anything less than strong authentication. In addition, there may be different authentication levels required to perform different operations. The most common example of this is someone who will accept no or simple authentication to allow "read" access to their entry, but requires simple or strong authentication to perform any modifications to their entry.

The authPolicy attribute is used on a per entry basis to provide this functionality. It divides access into three categories: modify, read and compare, and search and list. For each category, an authentication policy can be specified. For example

```
authp= strong # simple # trust
```

requires strong authentication for modification operations, simple authentication for read and compare operations, and no authentication for list and search operations on the entry.

The default behavior is as if every entry had the following authPolicy attribute:

```
authp= simple # simple # simple
```

which requires simple authentication for all operations.

Normally the authPolicy attribute will be inherited throughout an entire subtree of entries.

Appendix E

ISODE Consortium

The ISODE Consortium is a not-for-profit cooperative enterprise, whose mission is to promote and develop the ISODE package of OSI (Open System Interconnection) applications, which has been used extensively in the research community. The ISODE Consortium will be able to evolve the ISODE software more rapidly than would be possible for any single member. This will be to the mutual benefit of members of the consortium, and will help to stimulate the market for OSI, which is key technology to enable open communication between and within organisations. Membership of the ISODE Consortium is open to any organisation in any country.

The ISODE Consortium releases of ISODE will be made exclusively available to the ISODE Consortium members or by purchase of products from ISODE Consortium members. Academic organisations, and not for profit or government organisations with research as their primary purpose, will be given zero cost access to the ISODE Consortium releases, on the basis of simply signing a licence with minimal administrative overhead. This builds on a major strength of the ISODE package by facilitating use of ISODE within the research community, whilst allowing ISODE to evolve as a product base.

The ISODE Consortium has mailing lists for bug reports relating to the ISODE Package. These are:

bug-quipu@isode.com	– bugs relating to QUIPU
bug-pp@isode.com	– bugs relating to PP
bug-isode@isode.com	– bugs relating to any other parts of ISODE

These lists are for the planned ISODE Consortium releases of ISODE.

Bug reports relating to the "ISODE-8.0" release of ISODE are welcome. Changes will be incorporated into the ISODE Consortium releases, and not released to the public domain.

Further information may be obtained from:-

ISODE Consortium
US Office, c/o MCC
P.O. Box 200195
Austin
TX 78720
USA
Phone: +1-(512)-338-3340
Fax: +1-(512)-338-3600
EMail: ic-info@isode.com

ISODE Consortium
European Office
P.O. Box 505
LONDON
SW11 1DX
UK
Phone: +44-71-223-4062
Fax: +44-71-223-3846
EMail: ic-info@isode.com

Appendix F

Operating System Requirements

This appendix contains a table of hardware platforms and operating systems this version of ISODE is believed to work on. This information is based upon reports sent to *bug-isode*. It is not known how accurate this table is.

Machine	OS	Stacks
???	BSD/386	TCP
CCUR 6000	RTU 5.0	TCP
CCUR 6000	RTU 6.0	TCP X25 CLNS
CDC 4000 Series	EP/IX 1.3.2 EP/IX 1.4.1	TCP CLNS X25
COMPAQ 386/25	SCO Unix 5.2	TCP
COMPAQ 386	BSD	TCP X25
Convex C120	ConvexOS 8.1	TCP
DEC Vax	2nd Berkeley Network rel	TCP X25 CLNS
DEC	DECnet-ULTRIX V5.0	TCP CLNS
DEC	Ultrix 3.1D Ultrix 4.0 Ultrix 4.1	TCP X25
DEC	Ultrix 4.2	TCP X25 CLNS
DEC	VMS v5.x	TCP X25
DG Avion	DGUX 4.30	TCP
Encore Multimax 3xx Encore Multimax 5xx	UMAX V 2.2h	TCP
Encore NP1	UTX/32 3.1a	TCP X25
Encore PN6000 Encore PN9000	UTX/32 2.1b	TCP X25

Machine	OS	Stacks
HP/9000/3xx	HP/UX 6.0 HP-UX 7.05 B	TCP
HP/9000/8xx	HP-UX 7.00	TCP X25
IBM 3090	AIX/370 1.2.1	TCP
IBM PS/2	AIX 1.2.1	TCP
IBM RS/6000	AIX 3.2	TCP X25
ICL	DRS/6000	TCP X25
Interactive	Interactive 5.4.0.3	TCP
Macintosh	A/UX 2.0.1	TCP
Macintosh	MacOS V6.x	TCP
Mips 4_52	ATT_V3_0	TCP
NCR 3400	SVR4 Unix	TCP
NeXT		TCP
ORION/Clipper		TCP
Olivetti LSX-3020	X/OS 2.1	TCP X25
Pyramid 9800 Pyramid MIS	OSx 5.1 (4.3BSD/SVR3.2)	TCP
SEQUENT	DYNIX V3.0.18	TCP
Silicon Graphics IRIS	IRIS 3.2.2	TCP
Silicon Graphics IRIS	IRIS 4.01	TCP
Solbourne Series 5/600	OS/MP 4.1	TCP
Sony News-1750	NEWS-OS 3.3 NEWS-OS 4.0c	TCP
Sony News-3250	System V.4	TCP
Sun4 Sun3	SunOS 4.1 SunOS 4.1.1 SunOS 4.1.2 SunOS 4.0.3c	TCP X25 CONS CLNS