The Akenti Access Control System: Attribute Certificate Generation[1]

(An Application of Public-key Infrastructure and Digitally Signed Certificates)

William E. Johnston[2], Srilekha Mudumbai, Mary Thompson

Information and Computing Sciences Division

Ernest Orlando Lawrence Berkeley National Laboratory

University of California

[1] This work is supported by the Director, Office of Energy Research, Office of Computation and Technology Research, Mathematical, Information, and Computational Sciences Division, of the U. S. Department of Energy under Contract No. DE-AC03-76SF00098 with the University of California

[2] wejohnston@lbl.gov, 510-486-5014, mudumbai@george.lbl.gov, mrt@george.lbl.gov - http://www-itg.lbl.gov

The Attribute Certificate Generation Process

The access control process consists of defining use-conditions and then ascribing attributes to people that meet those use-conditions. A common use-condition will be that access is allowed if a person is a member of a named group. Under this circumstance, anyone who is authorized to convey the attribute “group_name” on a person may allow or deny access to a resource. Therefore, a data / resource owner may enable access rights (or remove them) by manipulating attribute certificates. The stakeholder (e.g. data owner) who establishes the use-conditions may determine who can issue certificates that provide group membership.

Akenti: Attribute Generation

An example use-condition certificate:

```
-----BEGIN TEXT CERTIFICATE-----
-----BEGIN TEXT-----
use-condition                                                          certificate type
issuerAndCA "/C=US/O=Lawrence Berkeley National
     Laboratory/OU=ICSD/CN=IDCG-CA" "/C=US/O=Lawrence Berkeley National
     Laboratory/OU=ICSD/CN=William E. Johnston sg1"                issuer of this cert
resource http://imglib.lbl.gov/shared/wej                         name of the resource
attribute "( group : HPSS )"                                        required attribute
scope sub-tree                                           scope of the access permission
enable access read,write,modify,chmod                                permitted actions
subjectCA"/C=US/O=Lawrence Berkeley National Laboratory/OU=ICSD/CN=IDCG-CA"
                                                                  CA required for user
attributeIssuerAndCA group Attribute "/C=US/O=Lawrence Berkeley National
     Laboratory/OU=ICSD/CN=IDCG-CA" "/C=US/O=Lawrence Berkeley National
     Laboratory/OU=ICSD/CN=William E. Johnston sg1"    name and naming authority
attributeIssuerAndCA group Attribute "/C=US/O=Lawrence Berkeley National
     Laboratory/OU=ICSD/CN=IDCG-CA" "/C=US/O=Lawrence Berkeley National
     Laboratory/OU=ICSD/CN=Mary R. Thompson sa2"
-----END TEXT-----
-----BEGIN SIGNATURE-----
```

Akenti: Attribute Generation

```
0lIsQ53O94OPX1/+dv8IwjQxf6MVntZRxeduGWsvaJSnP2RpHTgsYXayln5EFILa
-----END SIGNATURE-----
-----END TEXT CERTIFICATE-----
```

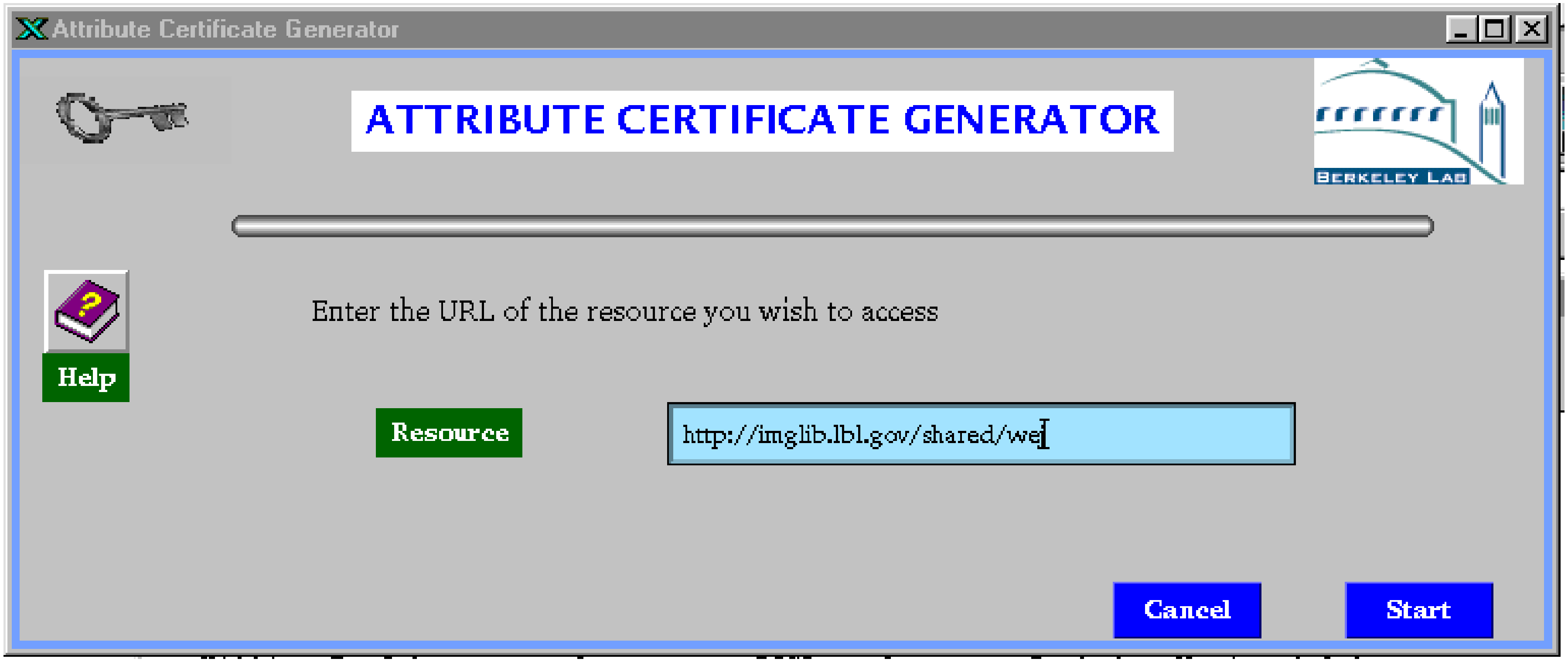
Akenti: Attribute Generation

A matching attribute certificate:

```
-----BEGIN TEXT ATTRIBUTE CERTIFICATE-----
-----BEGIN TEXT-----
attribute-certificate
attribute group
value HPSS
notValidBefore 980117223822Z
notValidAfter 980117233822Z
subject "/C=US/O=Lawrence Berkeley National
    Laboratory/OU=ICSD/UID=johnston/CN=William E. Johnston -
    u3-maat/Email=johnston@george" "/C=US/O=Lawrence Berkeley National
    Laboratory/OU=ICSD/CN=IDCG-CA"
issuer "/C=US/O=Lawrence Berkeley National Laboratory/OU=ICSD/CN=William E.
    Johnston sg1" "/C=US/O=Lawrence Berkeley National
    Laboratory/OU=ICSD/CN=IDCG-CA"
-----END TEXT-----
-----BEGIN SIGNATURE-----
otVDc2pwR9Bg5SPwmkZa5Dn8yrHuOoBHUBMop4rl4J0LNl36Q6xB9rdY2txP9wwd
-----END SIGNATURE-----
-----END TEXT ATTRIBUTE CERTIFICATE-----
```

5 6 7 8 9 10 11 12 13

Akenti: Attribute Generation



Attribute Certificate Generator
ATTRIBUTE CERTIFICATE GENERATOR
BERKELEY LAB
Help
Cancel
Start

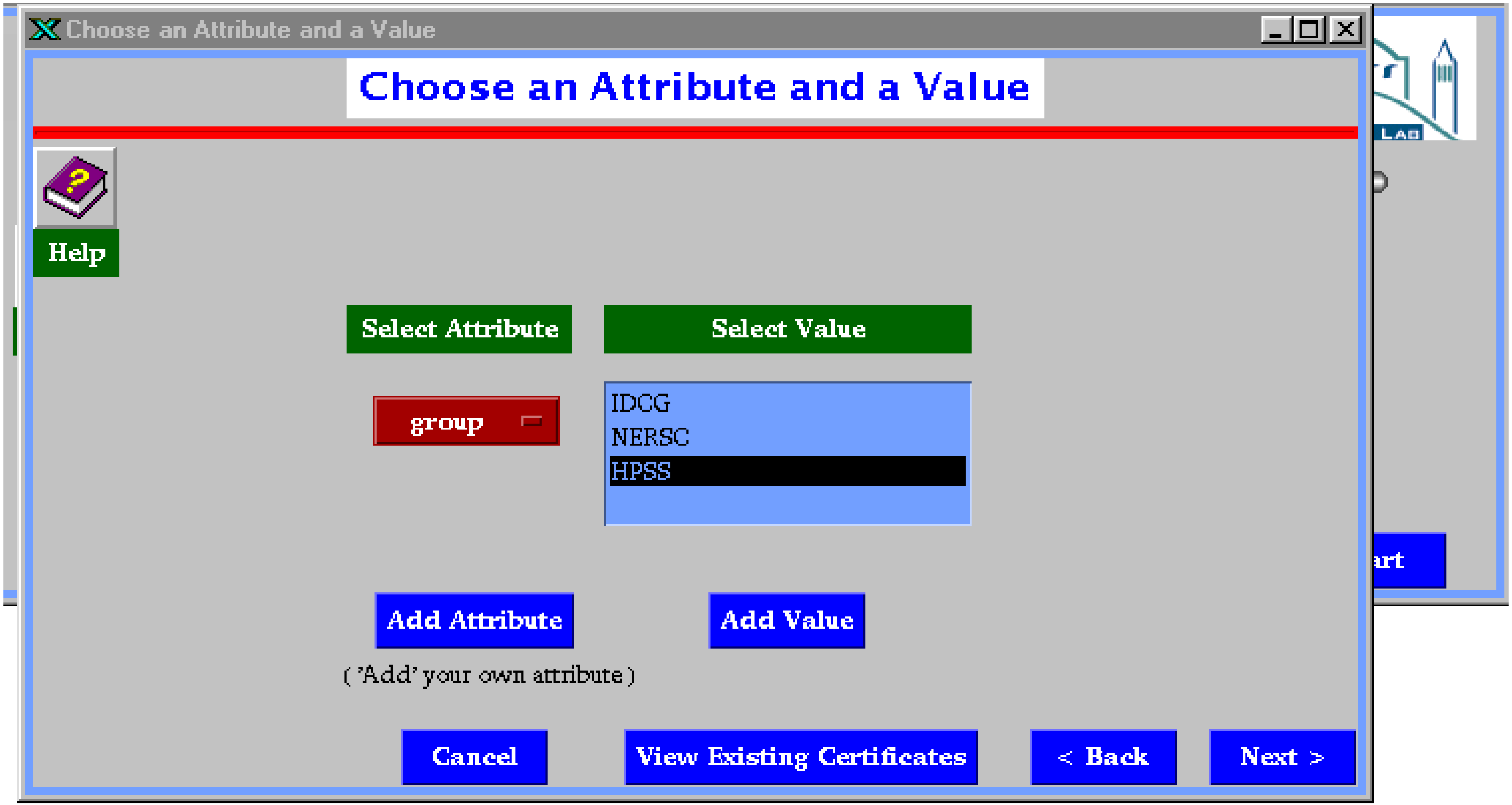
Enter the URL of the resource you wish to access

Resource: http://imglib.lbl.gov/shared/we

Specify the name of the resource.

Although user attributes don’t necessarily have anything to do with resources, the names of attributes that apply to a collection of resources (e.g. the directories of a project Web server) can be agreed on and provided as a guideline (and a template) for constructing attribute certificates.

Akenti: Attribute Generation

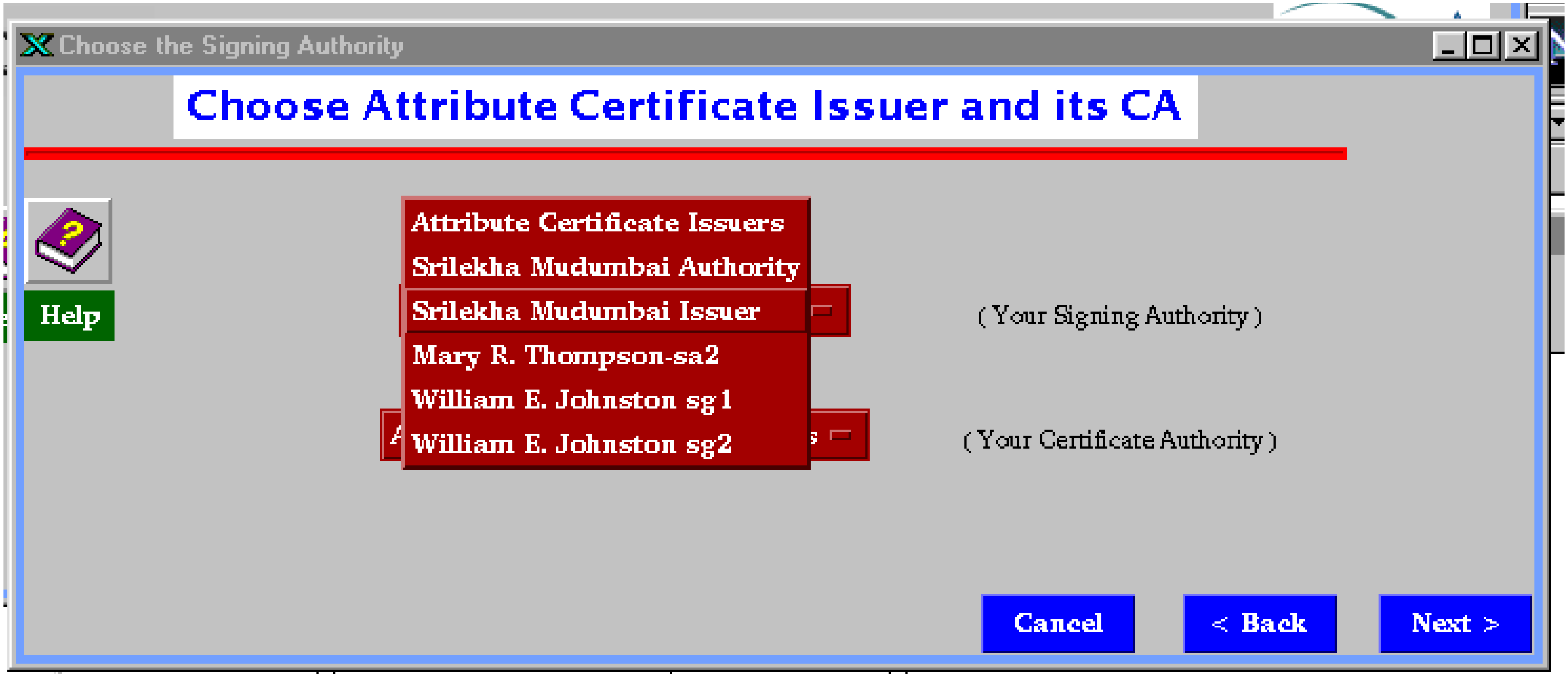


Choose an Attribute and a Value
Choose an Attribute and a Value
Help
Select Attribute
Select Value
group
IDCG
NERSC
HPSS
Add Attribute
Add Value
('Add' your own attribute)
Cancel
View Existing Certificates
< Back
Next >
LAB
art

The attribute name is "group", its value is to be specified.

The attribute issuer is not constrained to using a name or value from the template. A database of the issuer's certificates is maintained for connivance.

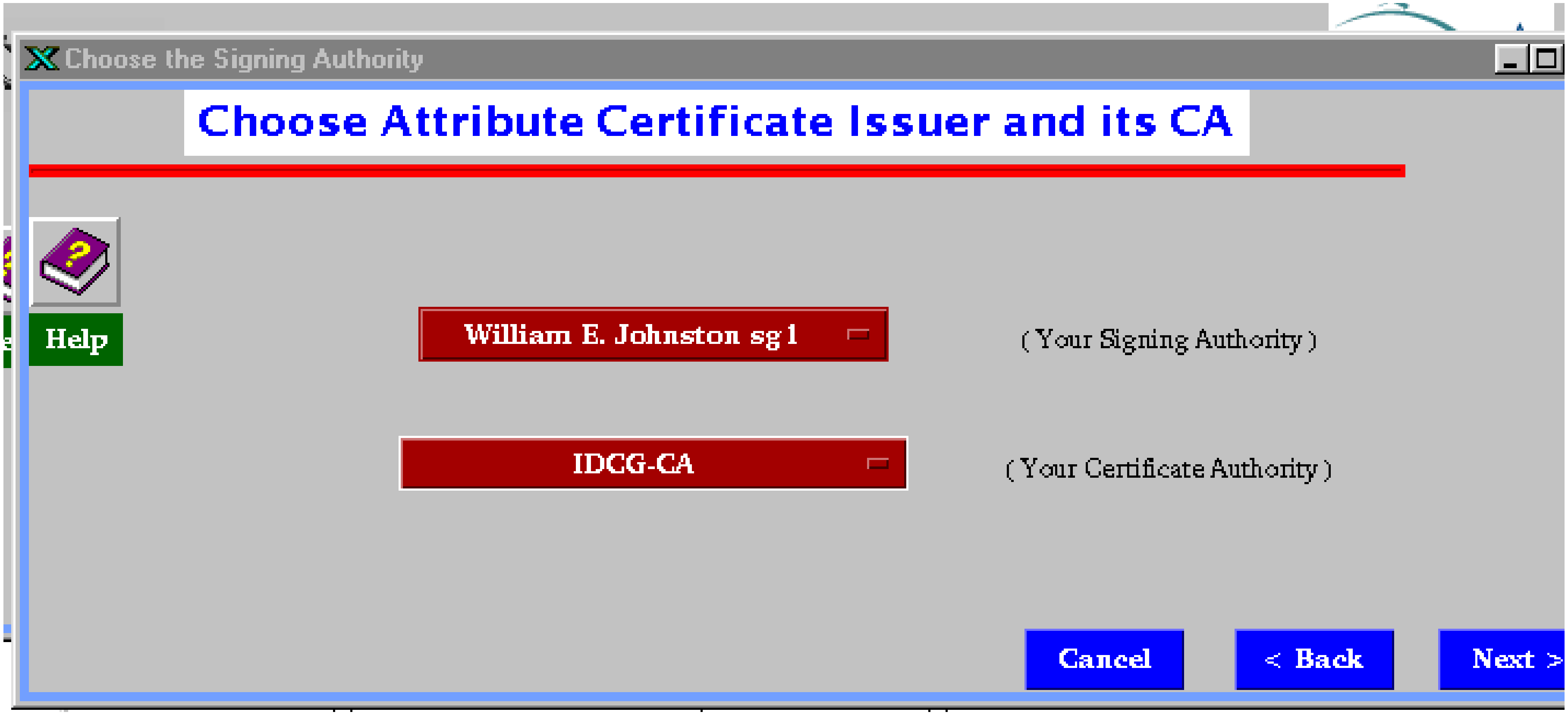
Akenti: Attribute Generation


Choose the Signing Authority
Choose Attribute Certificate Issuer and its CA
Help
Attribute Certificate Issuers
Srilekha Mudumbai Authority
Srilekha Mudumbai Issuer
Mary R. Thompson-sa2
William E. Johnston sg1
William E. Johnston sg2
(Your Signing Authority)
(Your Certificate Authority)
Cancel
< Back
Next >

The attribute issuer must be one of those specified in the use-condition.

In many environments, a separate identity is maintained for authentication and signing. The signing identity is used only for that purpose, and thus may be less vulnerable to attack and compromise.

Akenti: Attribute Generation



Choose the Signing Authority

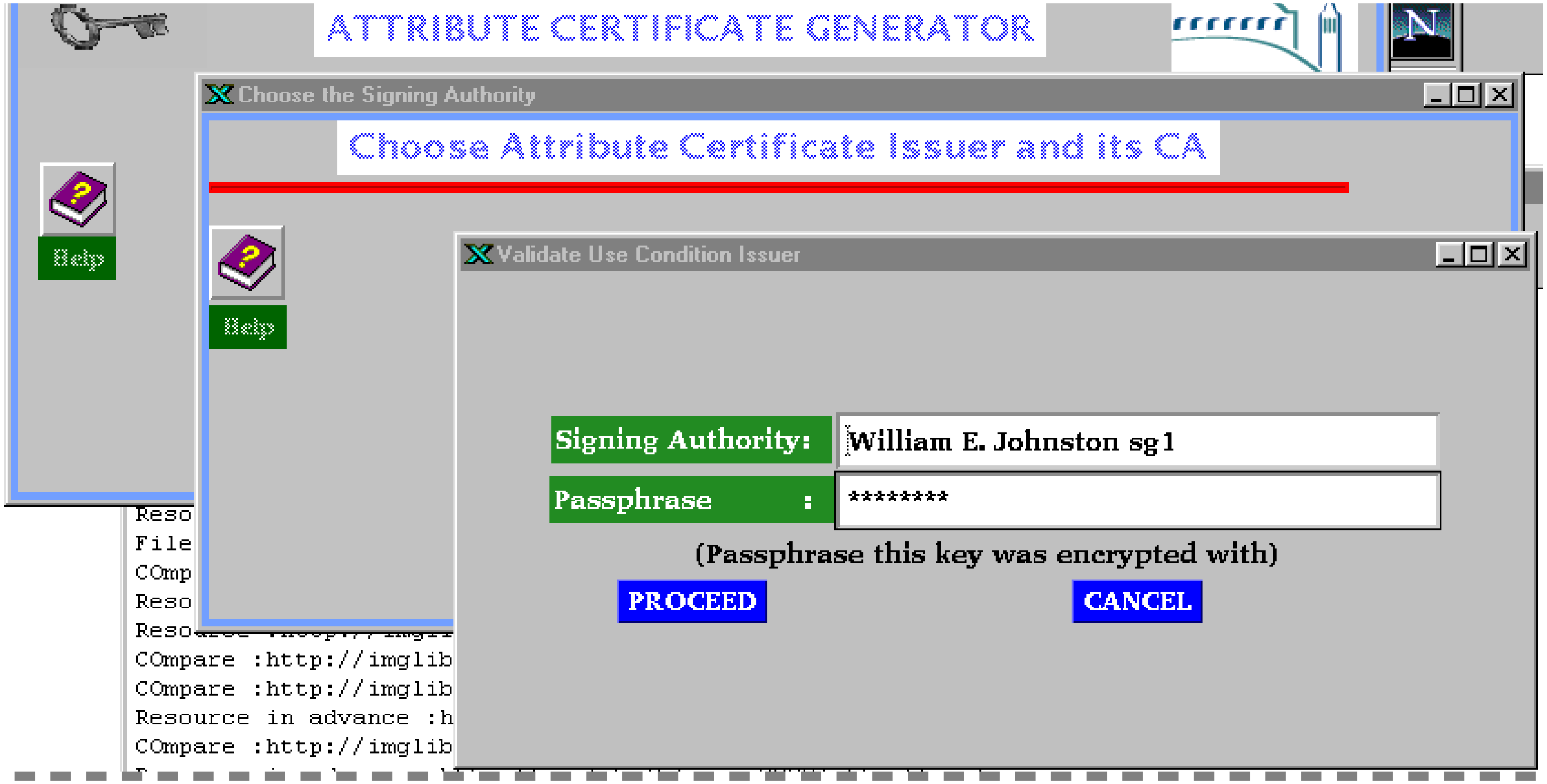
Choose Attribute Certificate Issuer and its CA

William E. Johnston sg1 (Your Signing Authority)

IDCG-CA (Your Certificate Authority)

The attribute issuer identity is established.

Akenti: Attribute Generation



ATTRIBUTE CERTIFICATE GENERATOR

Choose the Signing Authority

Choose Attribute Certificate Issuer and its CA

Validate Use Condition Issuer

Signing Authority: William E. Johnston sg1

Passphrase : ********

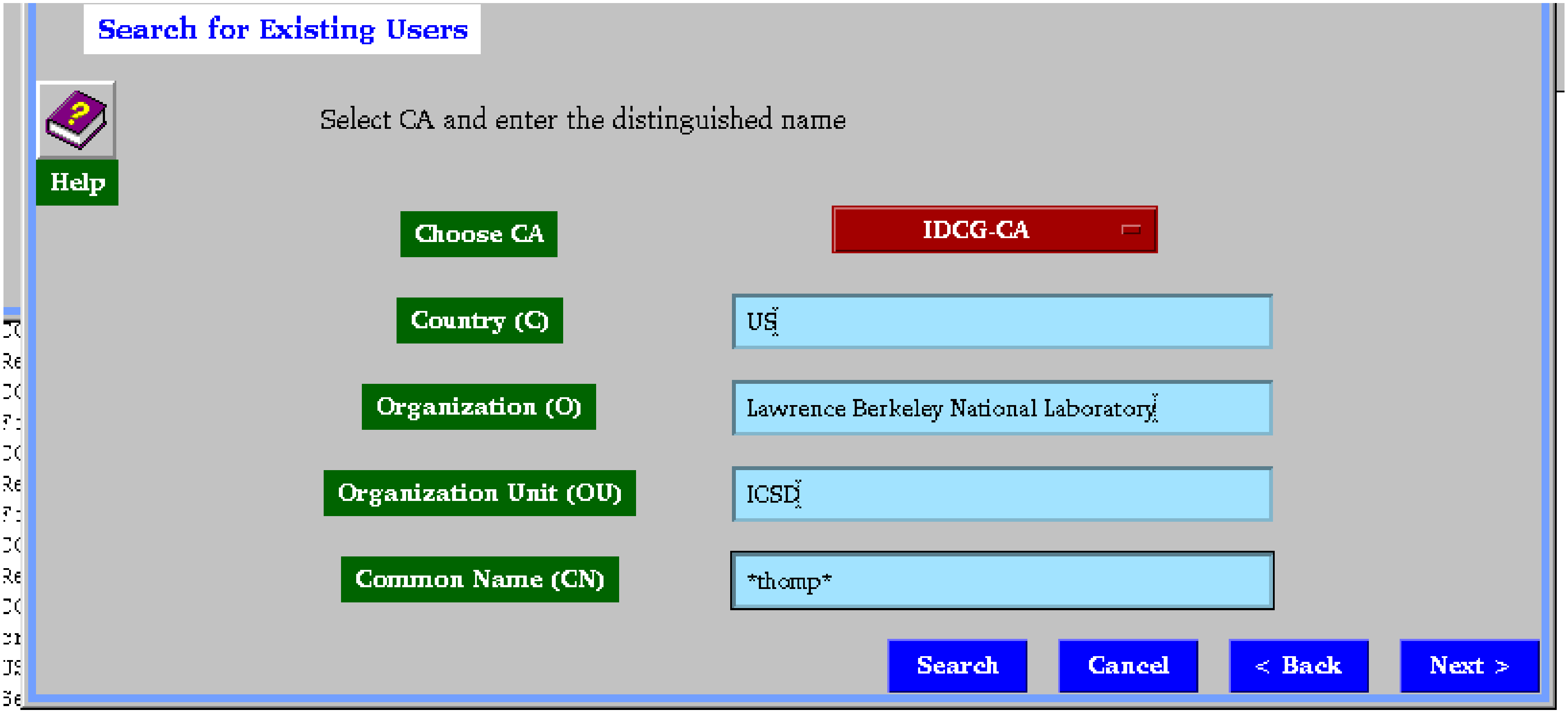
(Passphrase this key was encrypted with)

```
Reso
File
COmp
Reso
Reso
COmpare :http://imglib
COmpare :http://imglib
Resource in advance :h
COmpare :http://imglib
```

The private key must be used for signing

Currently, we have to create the signing identity outside of the Netscape browser in order to have access to the private key for signing documents like attribute certificates. (We may use the Java code signing tools in the future.) In any event, a certificate for the signing identity is issued by the CA.

Akenti: Attribute Generation



Search for Existing Users

Select CA and enter the distinguished name

Choose CA: IDCG-CA

Country (C): US

Organization (O): Lawrence Berkeley National Laboratory

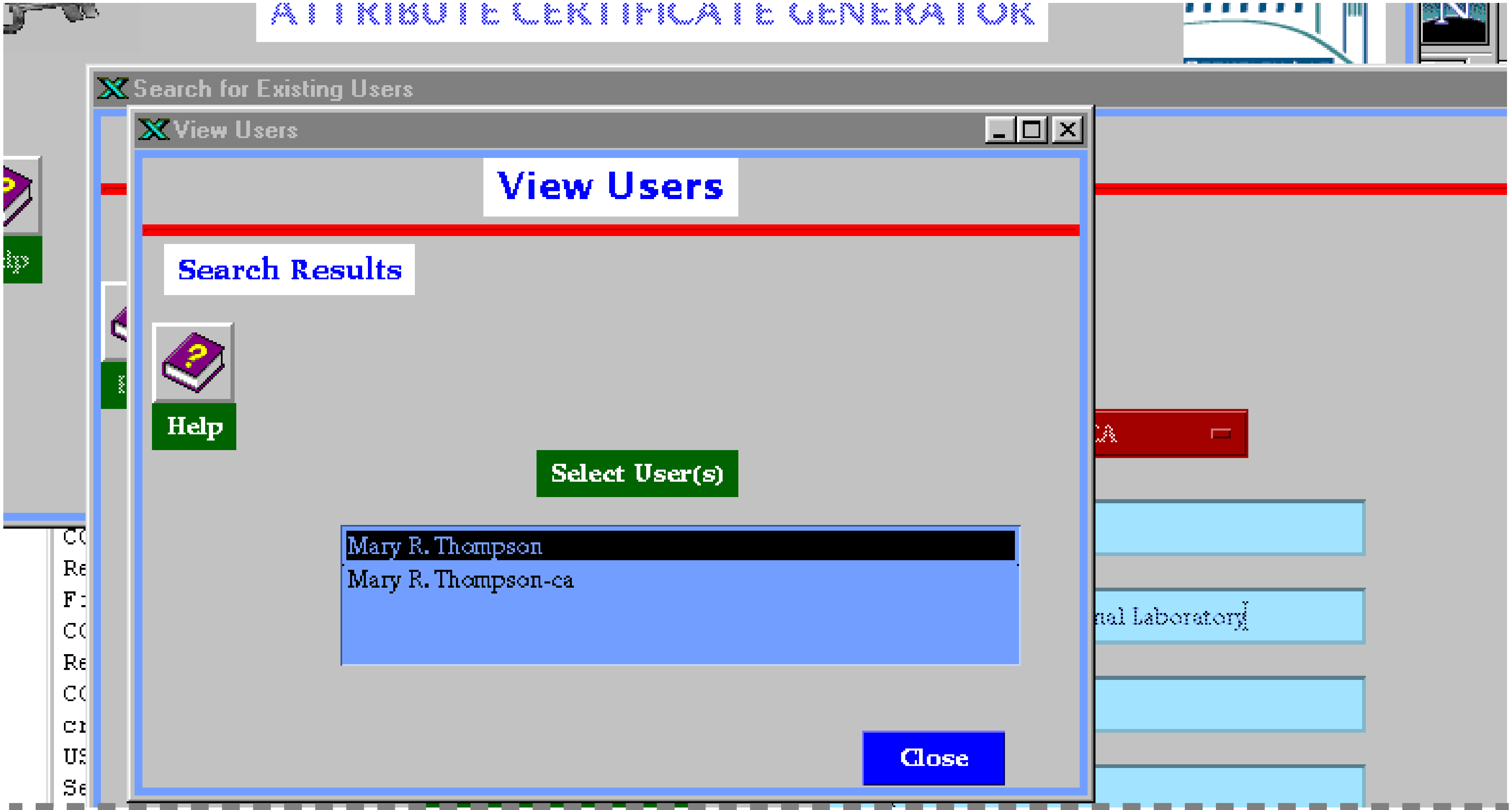
Organization Unit (OU): ICSD

Common Name (CN): *thomp*

The subject of the attribute certificate (the user) must be registered with a Certification Authority.

CA's provide a directory of known users. The access control is based on user identity as represented by a CA. This interface allows you to search the CA directory for particular users.

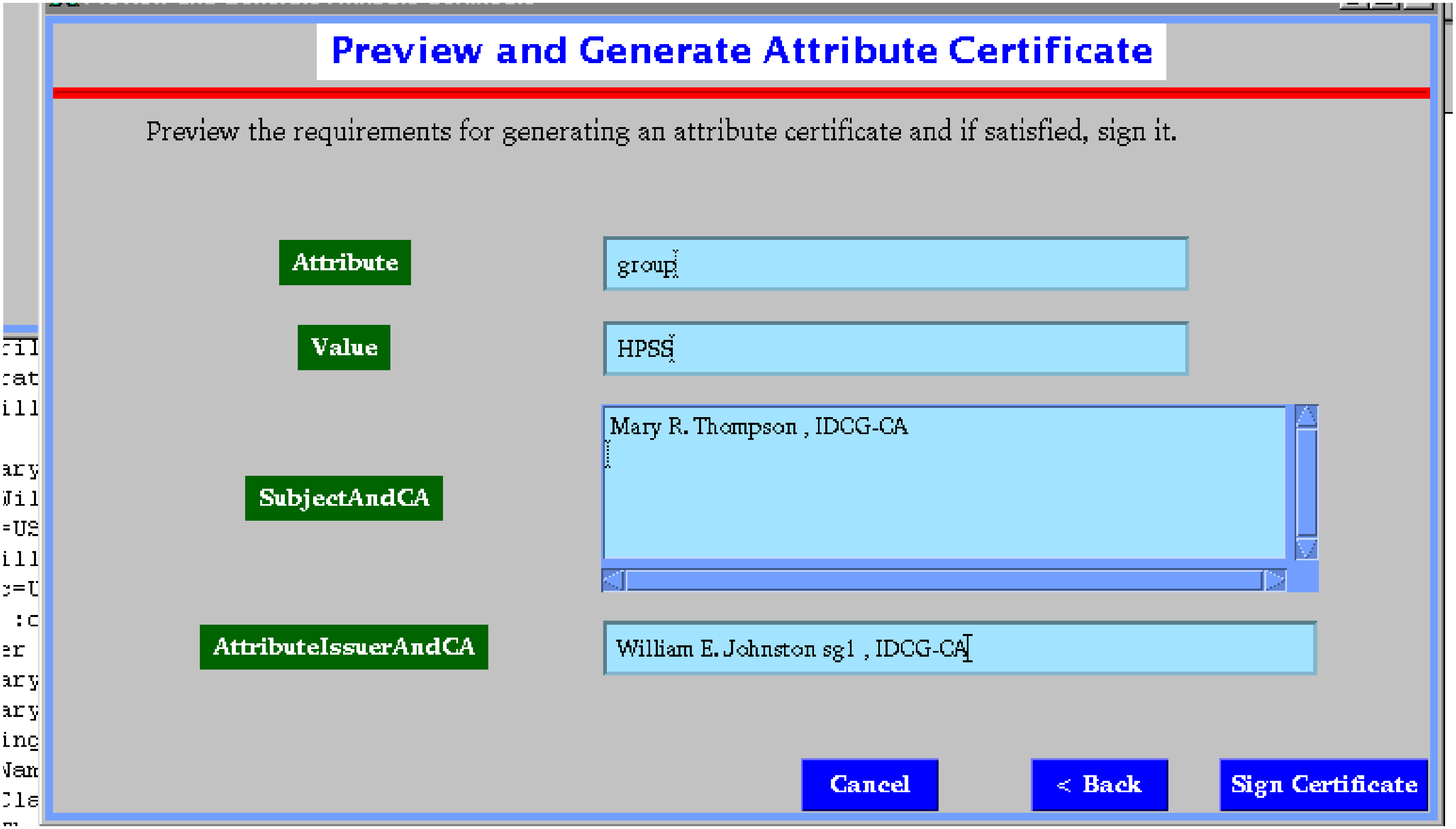
Akenti: Attribute Generation



Mary R. Thompson
Mary R. Thompson-ca

Select the user to certify.

Akenti: Attribute Generation



Preview and Generate Attribute Certificate

Preview the requirements for generating an attribute certificate and if satisfied, sign it.

Attribute: group

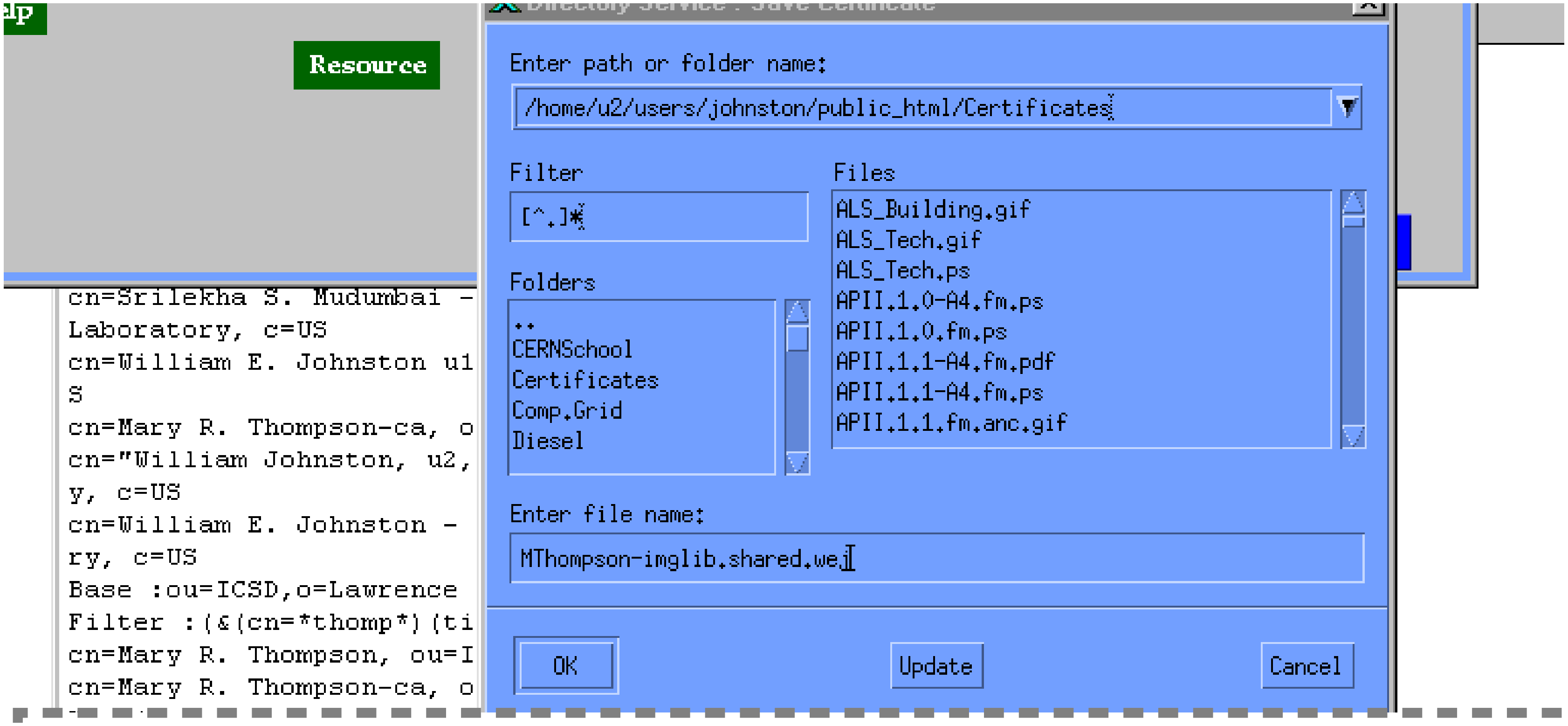
Value: HPSS

SubjectAndCA: Mary R. Thompson , IDCG-CA

AttributeIssuerAndCA: William E. Johnston sg1 , IDCG-CA

The certificate is constructed and signed.

Akenti: Attribute Generation



```
cn=Srilekha S. Mudumbai -
Laboratory, c=US
cn=William E. Johnston u1
S
cn=Mary R. Thompson-ca, o
cn="William Johnston, u2,
y, c=US
cn=William E. Johnston -
ry, c=US
Base :ou=ICSD,o=Lawrence
Filter :(&(cn=*thomp*)(ti
cn=Mary R. Thompson, ou=I
cn=Mary R. Thompson-ca, o
```

Enter path or folder name:
/home/u2/users/johnston/public_html/Certificates

Filter
[^.]*

Folders
..
CERNSchool
Certificates
Comp.Grid
Diesel

Files
ALS_Building.gif
ALS_Tech.gif
ALS_Tech.ps
APII.1.0-A4.fm.ps
APII.1.0.fm.ps
APII.1.1-A4.fm.pdf
APII.1.1-A4.fm.ps
APII.1.1.fm.anc.gif

Enter file name:
MThompson-imglib.shared.we

The certificate is “published”.

The location of attribute certificates is an important part of the assurance process. The signing authority must designate one or more trusted servers for publishing attribute certificates. These servers are “trusted” not because a certificate can be counterfeited (extremely difficult - impossible with ordinary resources - because of the cryptographic strength of public-key cryptography) but because the absence of a certificate from the designated server (usually the certifier’s Web server) denies access.