

The Akenti Access Control System: User Interaction¹

William E. Johnston², 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>

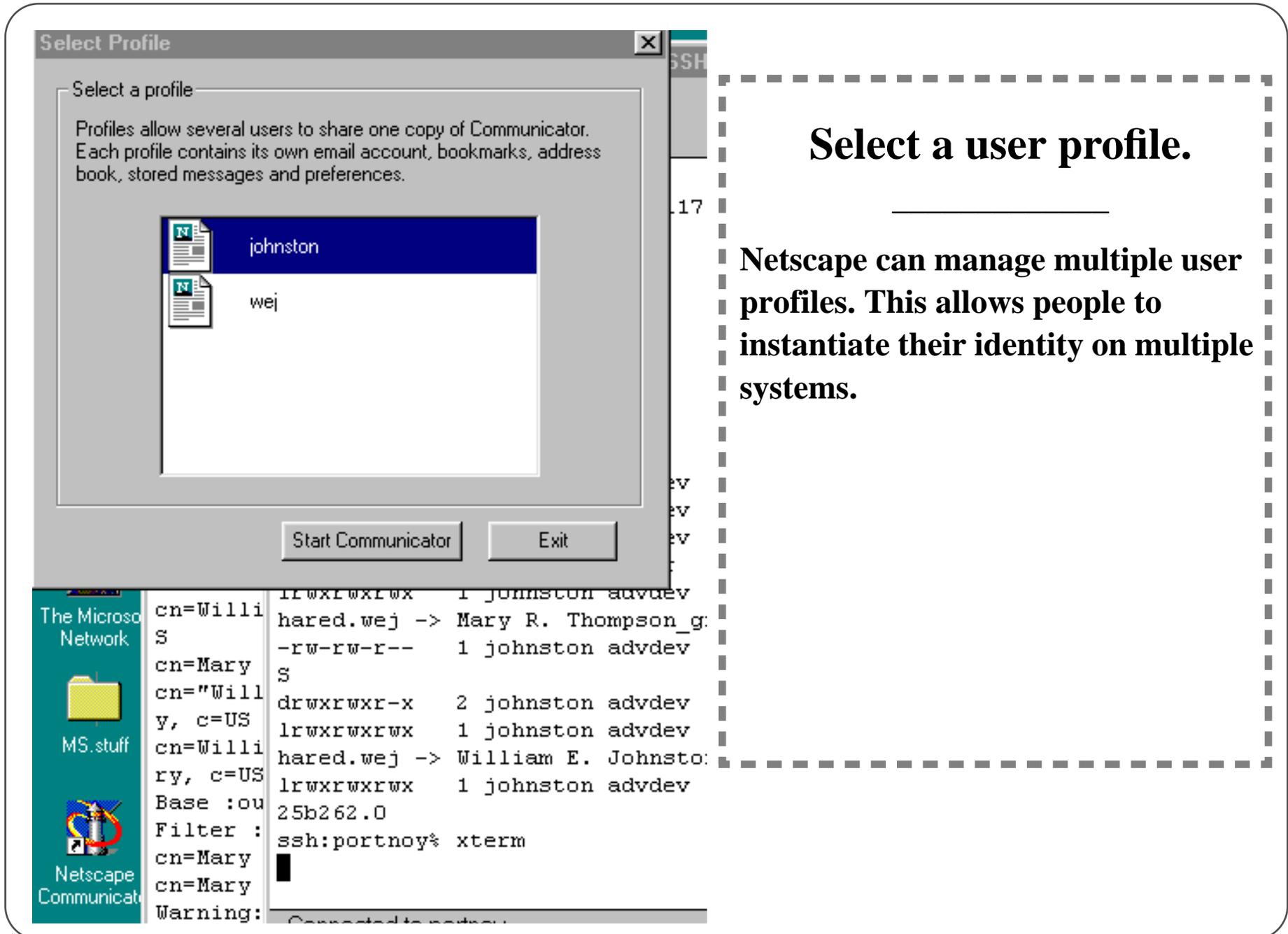
The Akenti User Interaction

The normal user interaction is intended to be as transparent as possible. When attempting to access a secure resource, the user client (e.g. a Web browser) supplies the private key to authenticate the user. The access control system identifies and obtains all of the required certificates: use-conditions for the resource and the corresponding user attributes. When the use-conditions are satisfied and the user identity authenticated, access is permitted with no user action other than making the private key available.

3-UI1 4 5 6-UI4a 7-UI3 8-UI4 9-UI5 10-UI8 11 12 13 14 15-UI-UC-cert 16-UI-attrib-cert 17-UI9-m1 18 19 - UI11 21 22



Akenti: User Interaction



The screenshot shows the Netscape Communicator interface. A 'Select Profile' dialog box is open, displaying two profiles: 'johnston' (selected) and 'wej'. Below the dialog, a terminal window shows the output of the 'ssh' command, listing users and their permissions. The terminal output is as follows:

```
110x110x110x 1 johnston advdev
hared.wej -> Mary R. Thompson_g:
-rw-rw-r-- 1 johnston advdev
S
drwxrwxr-x 2 johnston advdev
lrwxrwxrwx 1 johnston advdev
hared.wej -> William E. Johnsto:
lrwxrwxrwx 1 johnston advdev
Base :ou
25b262.0
Filter :
ssh:portnoy% xterm
Warning: Connected to portnoy:
```

Select a user profile.

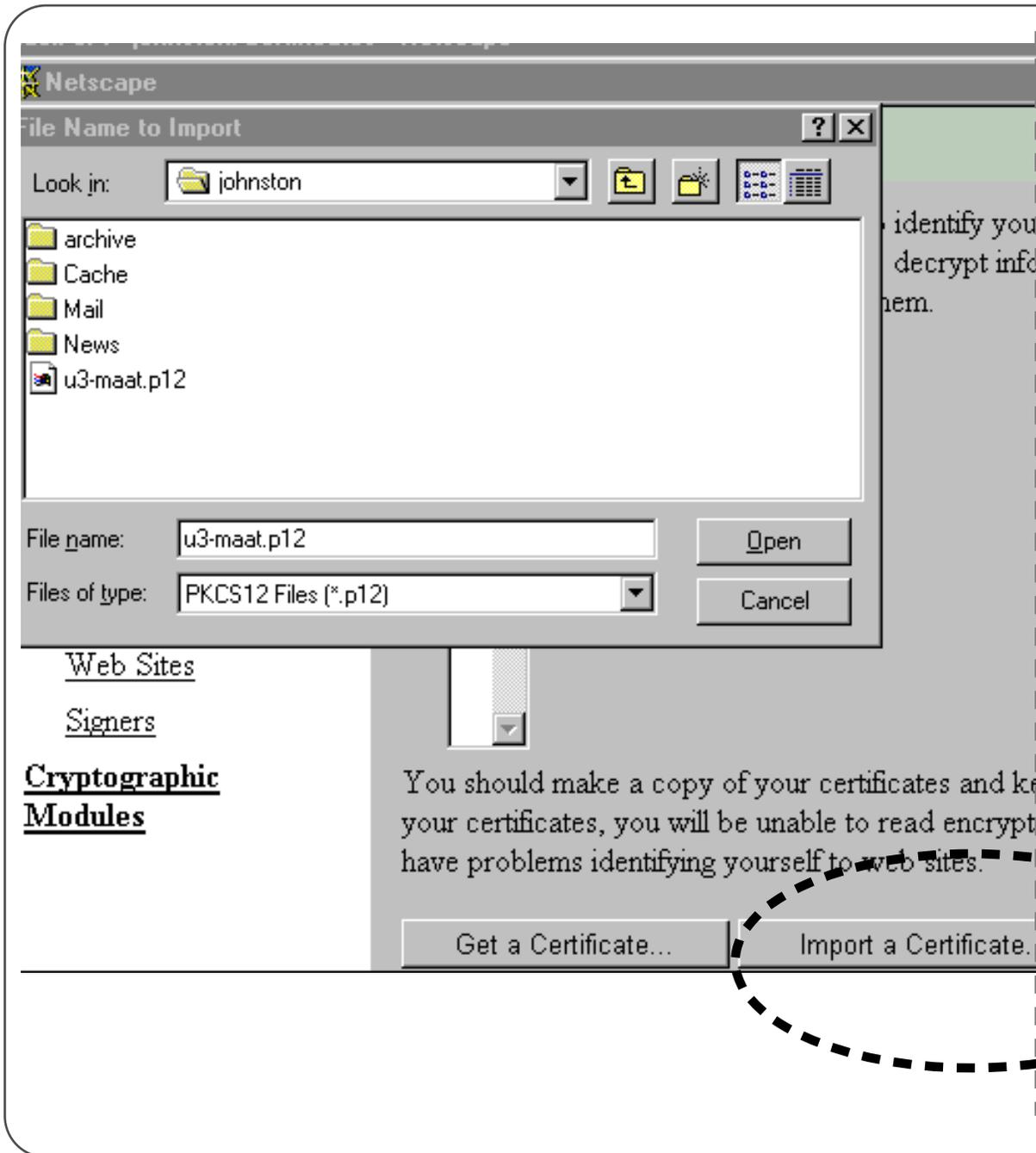
Netscape can manage multiple user profiles. This allows people to instantiate their identity on multiple systems.



Akenti: User Interaction

New user certificates (identities) may be acquired from a Certification Authority or imported to a user profile.

Your identity certificates may be exported and saved on a floppy, or even kept on your Web page, and imported to another browser. (Your identity - the “.p12” file - is encrypted when you export it from a browser.)



Akenti: User Interaction

The first time that an identity is imported to a user profile, a certificate database is established for that profile.

This database should be passphrase protected.

WRITE DOWN YOUR PASSPHRASE AND KEEP IT IN YOUR WALLET OR ADDRESS BOOK!

Get a Certificate... Import a Certificate...

Setting Up Your Communicator Password - Netscape

It is strongly recommended that you protect your Private Key with a Communicator password. If you want a password, leave the password field blank.

The safest passwords are at least 8 characters long, include both letters and numbers, and contain r from a dictionary.

Password: *****

Type it again to confirm: *****

Important: Your password cannot be recovered. If you forget it, you will lose all of your certificate.

If you wish to change your password or other security preferences, choose Security Info from the Communicator menu.

More Info... OK Cancel



Akenti: User Interaction

Your Certificates

Security Info
Passwords
Navigator
Messenger
Java/JavaScript
Certificates
 Yours
 People
 Web Sites
 Signers
Cryptographic Modules

You can use any of these certificates to identify yourself to other people and to web sites. Communicator uses your certificates to decrypt information sent to you. Your certificates are signed by the organization that issued them.

These are your certificates:

William E. Johnston - maat.lbl.gov's Lawrence Berkeley National Laboratory ID	View
William E. Johnston u1's Lawrence Berkeley National Laboratory ID	Verify
	Delete
	Export

You should make a copy of your certificates and keep them in a safe place. If you ever lose your certificates, you will be unable to read encrypted mail you have received, and you may have problems identifying yourself to web sites.

If you have more than one identity, you must select the one relevant to this resource.

The use-conditions for resources are given, directly or indirectly, in terms of the X.509 identity certificates issued by your Certification Authority. These certificates are kept both in your browser database and in the certificate server of the CA (which is where they are obtained when authenticating your identity.)



Akenti: User Interaction

Access a secure server.

Secure Web servers use the SSL (Secure Sockets Layer) protocol to authenticate the client and the server, and for setting up an encrypted communication channel. *https* refers to Web servers that use the SSL protocol.

LBL Data Intensive Distributed Computing Research Group and Imaging and Collaboration Group

File Edit View Go Communicator Help

Back Forward Reload Home Search Guide Print Security Stop

Bookmarks Location: <http://www.itg.lbl.gov/>

Instant Message Internet Lookup New&Cool

Data Intensive Distributed Computing Research and Imaging and Distribution Collaboration Group

NERSC and Information and Computing Sciences: Ernest Orlando Lawrence Berkeley One Cyclotron Road, 50B-2270, Berkeley, CA 94720-8080

This page summarizes the activities of the Imaging and Distribution Collaboration Group. A marker like this  indicates that within one or two hops you'll find an **interactive** resource like the Whole Frog Project where you can experience the benefits that imaging and networking bring to science, education, and industry.

Open Page

Enter the World Wide Web location (URL) or specify the local file you would like to open:

<https://imglib.lbl.gov/shared> Choose File...

Open location or file in: Composer Navigator

Open Cancel Help



Akenti: User Interaction

**Make your identity
available for
authentication.**

When a remote server requests your identity you must “unlock” your private key so that it may be used to authenticate your identity. (Recall that your identity is authenticated by checking that your private key and your published public key match.) Netscape allows several options for when your passphrase is requested, but at the very least it is always requested the first time that you are authenticated.

ive Distributed Computing Research Group and Imaging and Distributed Collaboration Gr -
Communicator Help
Reload Home Search Guide Print Security Stop
Location: http://www.itg.lbl.gov/
Internet Lookup New&Cool

**Data Intensive Distributed
Computing Research Group
and
Imaging and Distributed**

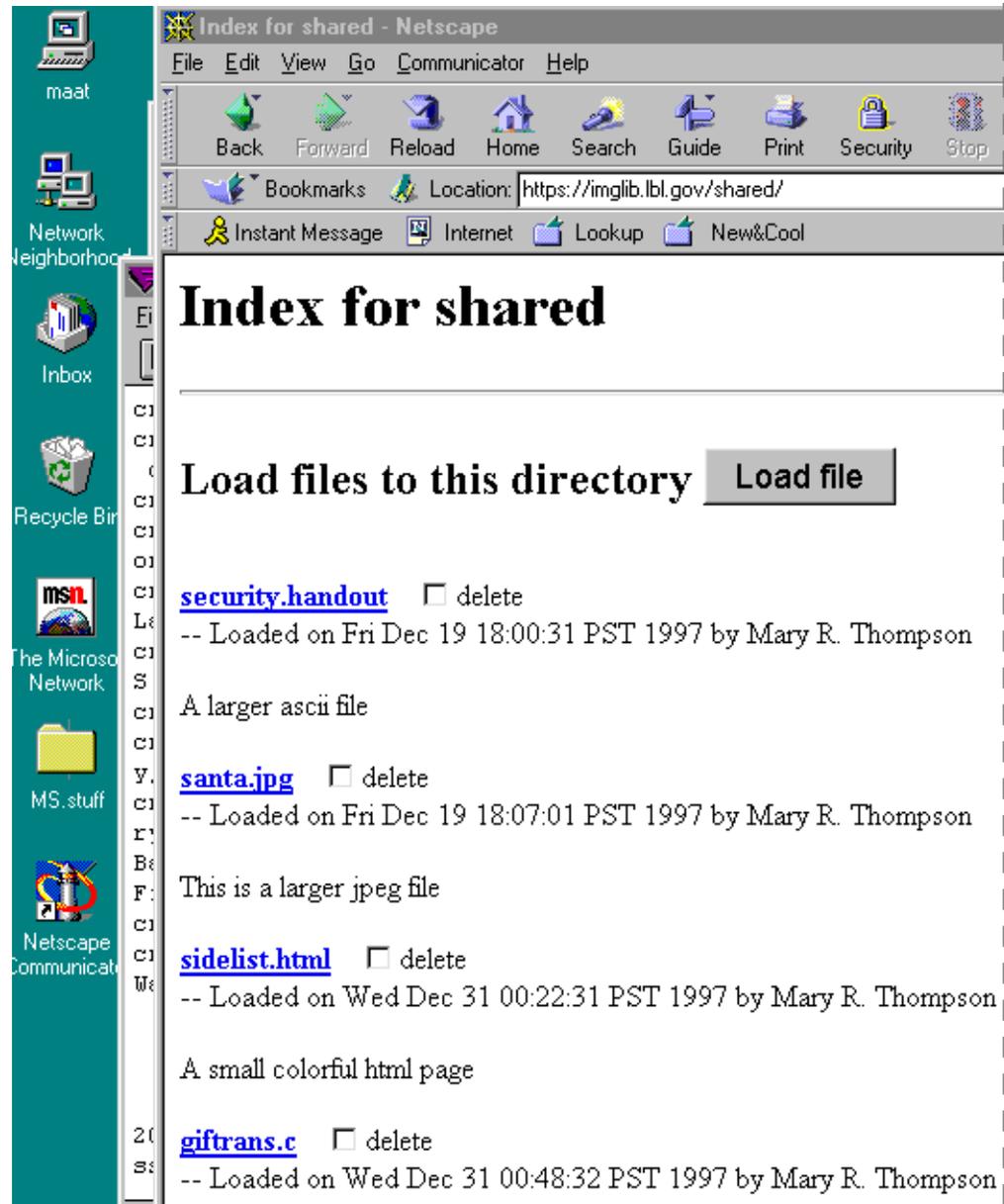
Computing Science
Lawrence Berkeley
oad, 50B-2270, Berkeley, CA, USA 94720

izes the activities of the Data Intensive Distributed Computing Research Group and I
oup. A marker like this  indicates that within one or two hops you'll find an interact

Password Entry Dialog
Please enter the password or the pin for
Communicator Certificate DB.
XXXXXXXXXX
OK Cancel



Akenti: User Interaction

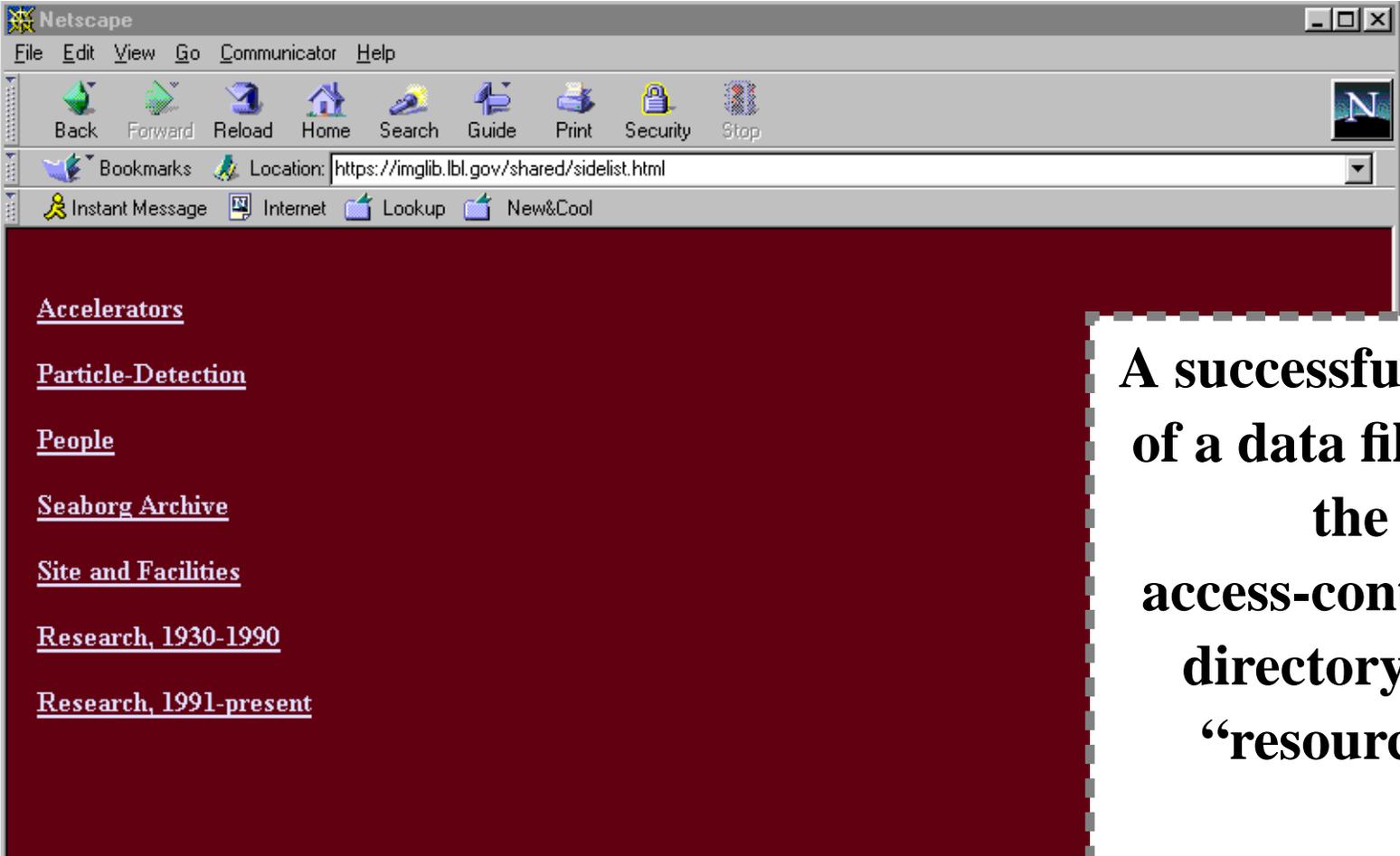


The user has met the use-conditions for this resource and access is allowed.

The “normal” operation of the access control system is intended to be transparent to the user, and specific use-conditions are not normally visible to the user. The use-conditions, and the user attributes needed to satisfy them, are established elsewhere. (However if “real” credentials beyond identity are required for a particular resource, then the user will have to provide those to the party who is certifying that user attribute.)



Akenti: User Interaction



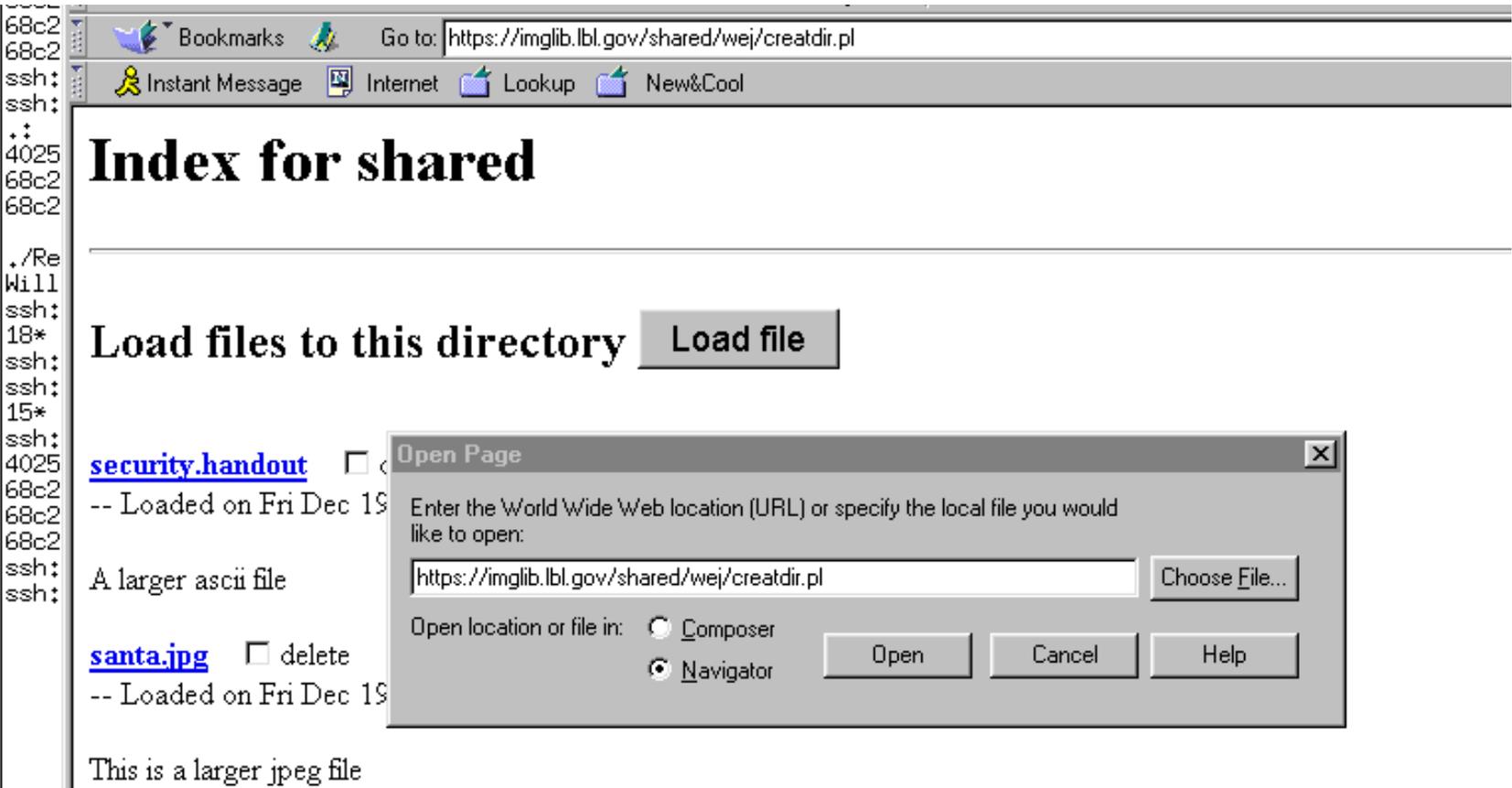
The screenshot shows a Netscape browser window with the following elements:

- Menu bar: File, Edit, View, Go, Communicator, Help
- Toolbar: Back, Forward, Reload, Home, Search, Guide, Print, Security, Stop
- Address bar: Location: <https://imglib.lbl.gov/shared/sidelist.html>
- Buttons: Instant Message, Internet, Lookup, New&Cool
- Main content area (dark red background):
 - [Accelerators](#)
 - [Particle-Detection](#)
 - [People](#)
 - [Seaborg Archive](#)
 - [Site and Facilities](#)
 - [Research, 1930-1990](#)
 - [Research, 1991-present](#)

A dashed box highlights the text: **A successful access of a data file from the access-controlled directory (the “resource”).**



Akenti: User Interaction



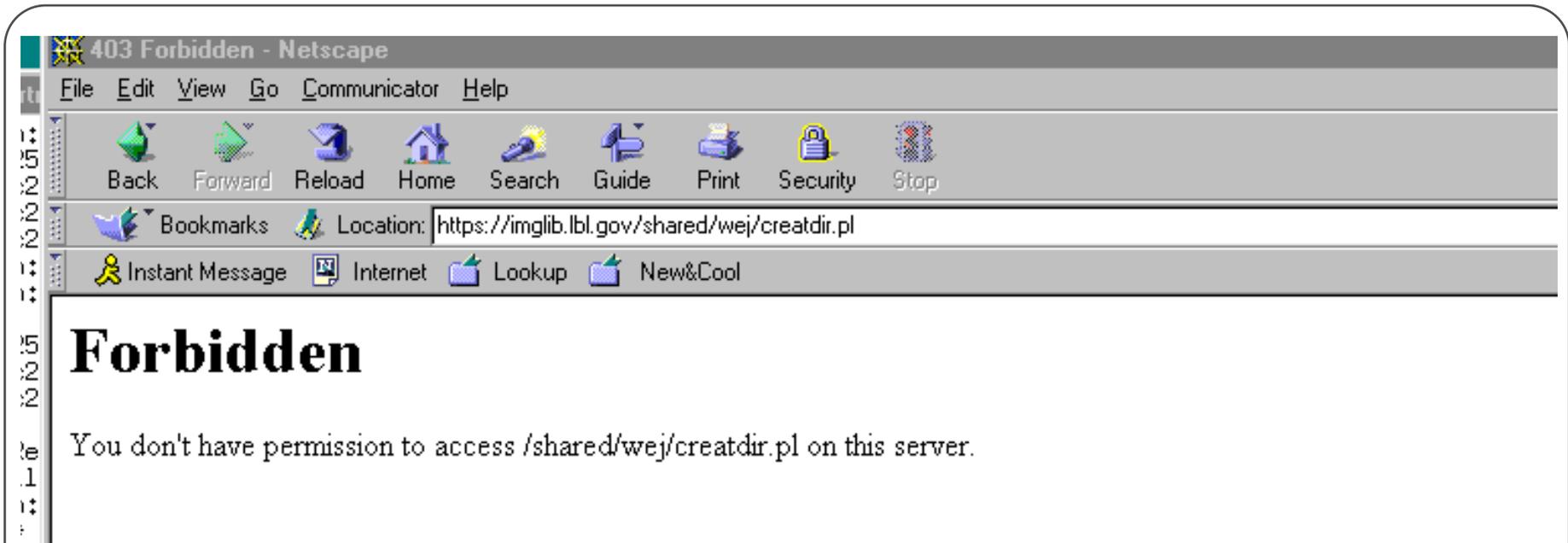
The screenshot shows a web browser window with the address bar containing `https://imglib.lbl.gov/shared/wej/creatdir.pl`. The page title is "Index for shared". Below the title, there is a button labeled "Load file" and the text "Load files to this directory". A list of files is displayed, including [security.handout](#) and [santa.jpg](#). An "Open Page" dialog box is open, showing the URL `https://imglib.lbl.gov/shared/wej/creatdir.pl` in the input field. The dialog box has buttons for "Choose File...", "Open", "Cancel", and "Help".

Attempted access to the “wej” sub-directory.

The “wej” sub-directory is a different resource, and has different stakeholders and use-conditions than “shared”.



Akenti: User Interaction

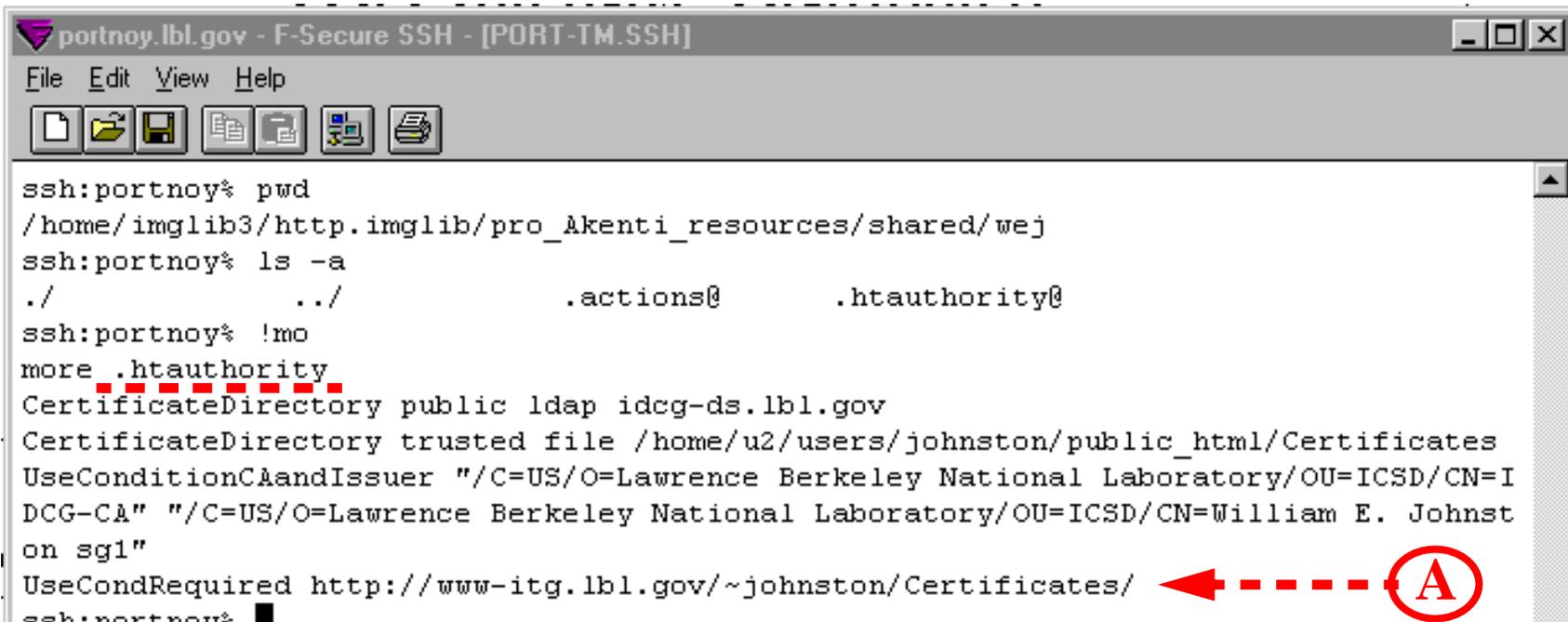


An attempted access to the “wej” sub-directory is rejected.

This means that a use-condition for this resource has not been met. Although this message is the same as that returned by the standard *htaccess* access control method, this Web server is using the Akenti access control. Future versions of Akenti will tell the user what use-condition has not been met. Currently, in order to find out why access was forbidden one has to know a little about how Akenti works.



Akenti: User Interaction



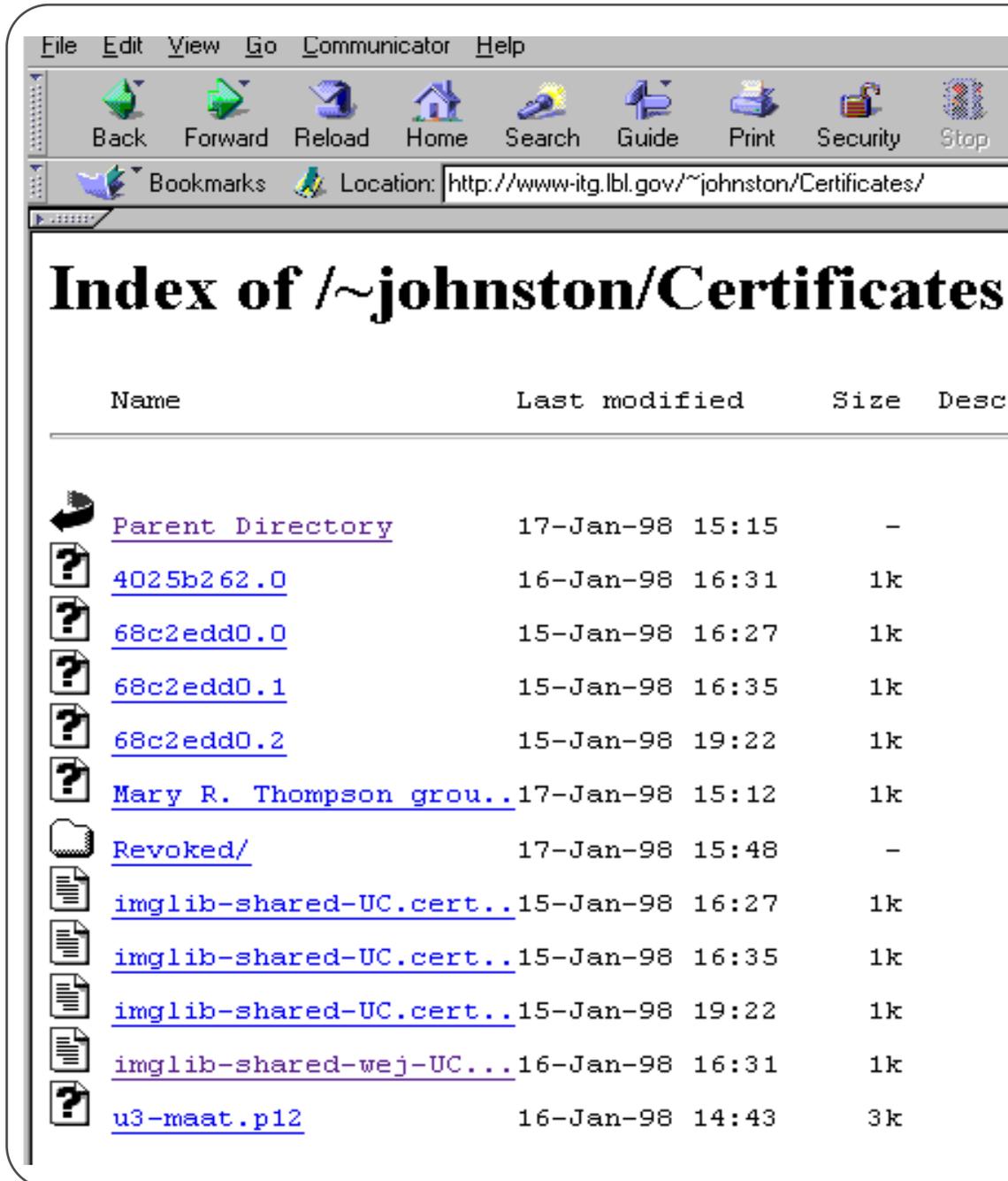
```
portnoy.lbl.gov - F-Secure SSH - [PORT-TM.SSH]
File Edit View Help
ssh:portnoy% pwd
/home/imglib3/http.imglib/pro_Akenti_resources/shared/wej
ssh:portnoy% ls -a
./          ../          .actions@   .htauthority@
ssh:portnoy% !mo
more .htauthority
CertificateDirectory public ldap idcg-ds.lbl.gov
CertificateDirectory trusted file /home/u2/users/johnston/public_html/Certificates
UseConditionC&andIssuer "/C=US/O=Lawrence Berkeley National Laboratory/OU=ICSD/CN=I
DCG-CA" "/C=US/O=Lawrence Berkeley National Laboratory/OU=ICSD/CN=William E. Johnst
on sgl"
UseCondRequired http://www-itg.lbl.gov/~johnston/Certificates/
ssh:portnoy% █
```

Each resource has a configuration file that defines the stakeholders.

In practical terms, the “stakeholders” are those who can impose use-conditions on a resource (e.g. the data owner). The use-conditions of all stakeholders must be satisfied before access is allowed. Currently the stakeholders, and where their use-conditions are located, are defined in a file that is managed by a “trusted third-party” - e.g. the Webmaster - and is called *.htauthority* .



Akenti: User Interaction



The screenshot shows a web browser window with the following elements:

- Menu bar: File, Edit, View, Go, Communicator, Help
- Navigation buttons: Back, Forward, Reload, Home, Search, Guide, Print, Security, Stop
- Address bar: Location: <http://www-itg.lbl.gov/~johnston/Certificates/>
- Page title: **Index of /~johnston/Certificates**
- Table with columns: Name, Last modified, Size, Descr

Name	Last modified	Size	Descr
Parent Directory	17-Jan-98 15:15	-	
4025b262.0	16-Jan-98 16:31	1k	
68c2edd0.0	15-Jan-98 16:27	1k	
68c2edd0.1	15-Jan-98 16:35	1k	
68c2edd0.2	15-Jan-98 19:22	1k	
Mary R. Thompson grou..	17-Jan-98 15:12	1k	
Revoked/	17-Jan-98 15:48	-	
imglib-shared-UC.cert..	15-Jan-98 16:27	1k	
imglib-shared-UC.cert..	15-Jan-98 16:35	1k	
imglib-shared-UC.cert..	15-Jan-98 19:22	1k	
imglib-shared-wej-UC...	16-Jan-98 16:31	1k	
u3-maat.p12	16-Jan-98 14:43	3k	

Use-condition certificates are maintained by the stakeholders.

Use-conditions are retrieved from the Web server of the stakeholders (as specified at “A”, above).



Akenti: User Interaction

```
<HTML>
<TITLE> Use-Condition Certificate </TITLE>
<BODY>
-----BEGIN TEXT CERTIFICATE-----
-----BEGIN TEXT-----
use-condition
issuerAndCA "/C=US/O=Lawrence Berkeley National Laboratory/OU=ICSD/CN=IDCG-CA" "/C=US/O=Lawrence Berkeley Nation
attribute "( group : HPSS )"
resource http://inglib.lbl.gov/shared/wej
scope sub-tree
enable access read,write,modify,chmod
subjectCA "/C=US/O=Lawrence Berkeley National Laboratory/OU=ICSD/CN=IDCG-CA"
attributeIssuerAndCA group Attribute "/C=US/O=Lawrence Berkeley National Laboratory/OU=ICSD/CN=IDCG-CA" "/C=US/O
-----END TEXT-----
-----BEGIN SIGNATURE-----
01IsQ530940PX1/+dv8IwjQxf6MVntZRxeduGWsvaJSnP2RpHTgsYXayln5EFILa
-----END SIGNATURE-----
-----END TEXT CERTIFICATE-----
</BODY>
```

The use-conditions are represented as digitally signed certificates.

The use-condition certificate identifies: the issuer (stakeholder); the resource; the required attribute; what identity authorities will be trusted, and finally; who is trusted to certify the required attribute. Currently the location of the attribute certificates is given in the *.htaauthority* file - in the future it will probably be included in the use-condition certificate where the certifiers are named.



Akenti: User Interaction

```
Mary R. Thompson_group_HPSS.cert          imglib-shared-wej-UC.cert.0.txt@
Revoked/                                  u3-maat.p12
ssh:portnoy% more "Mary R. Thompson_group_HPSS.cert"
-----BEGIN TEXT ATTRIBUTE CERTIFICATE-----
-----BEGIN TEXT-----
attribute-certificate
attribute group
value HPSS
notValidBefore 980117231245Z
notValidAfter 980118001245Z
subject "/C=US/O=Lawrence Berkeley National Laboratory/OU=ICSD/UID=mrt/CN=Mary R
. Thompson/Email=mrthompson@lbl.gov"
"/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. John
ston sg1" "/C=US/O=Lawrence Berkeley
National Laboratory/OU=ICSD/CN=IDCG-CA"
-----END TEXT-----
-----BEGIN SIGNATURE-----
r+DjgKg/QKmpEU9XmiYTj1YzAp/ZmvOvq4psVBCMT1XVKIYjvO5b2Me9rDh5ZMwz
-----END SIGNATURE-----
-----END TEXT ATTRIBUTE CERTIFICATE-----
ssh:portnoy% █
```

The attributes are represented as digitally signed certificates.

The attribute certificate identifies: the attribute being attested to; the “subject” who possesses the attribute, and; the issuer (the trusted attribute certifier).



Akenti: User Interaction

```
ssh:portnoy% pwd
/home/u2/users/johnston/public_html/Certificates ←
ssh:portnoy% ls -R
.:
4025b262.0          Mary R. Thompson_group_HPSS.cert  imglib-shared-UC.cert.2.txt@
68c2edd0.0          Revoked/                          imglib-shared-wej-UC.cert.0.txt@
68c2edd0.1          imglib-shared-UC.cert.0.txt@      u3-maat.p12
68c2edd0.2          imglib-shared-UC.cert.1.txt@

./Revoked:
William E. Johnston - u3-maat_group_HPSS.cert
ssh:portnoy%
ssh:portnoy% cd Revoked
18* /home/u2/users/johnston/public_html/Certificates/Revoked
ssh:portnoy% mv "William E. Johnston - u3-maat_group_HPSS.cert" ..
ssh:portnoy% cd ..
15* /home/u2/users/johnston/public_html/Certificates
ssh:portnoy% ls -R
.:
4025b262.0          William E. Johnston - u3-maat_group_HPSS.cert ←
68c2edd0.0          imglib-shared-UC.cert.0.txt@
68c2edd0.1          imglib-shared-UC.cert.1.txt@
68c2edd0.2          imglib-shared-UC.cert.2.txt@
Mary R. Thompson_group_HPSS.cert  imglib-shared-wej-UC.cert.0.txt@
Revoked/              u3-maat.p12

./Revoked:
ssh:portnoy% █
```

The require attribute is revoked (since it is not in the specified location, it is not visible to the access control system.)

In this case the attribute certificate has been previously generated, so to enable access it must just be placed into the location where Akenti expects it to be.



Akenti: User Interaction

Index of /shared/wej - Netscape

File Edit View Go Communicator Help

Back Forward Reload Home Search Guide Print Security Stop

Bookmarks Location: https://imglib.lbl.gov/shared/wej/

Instant Message Internet Lookup New&Cool

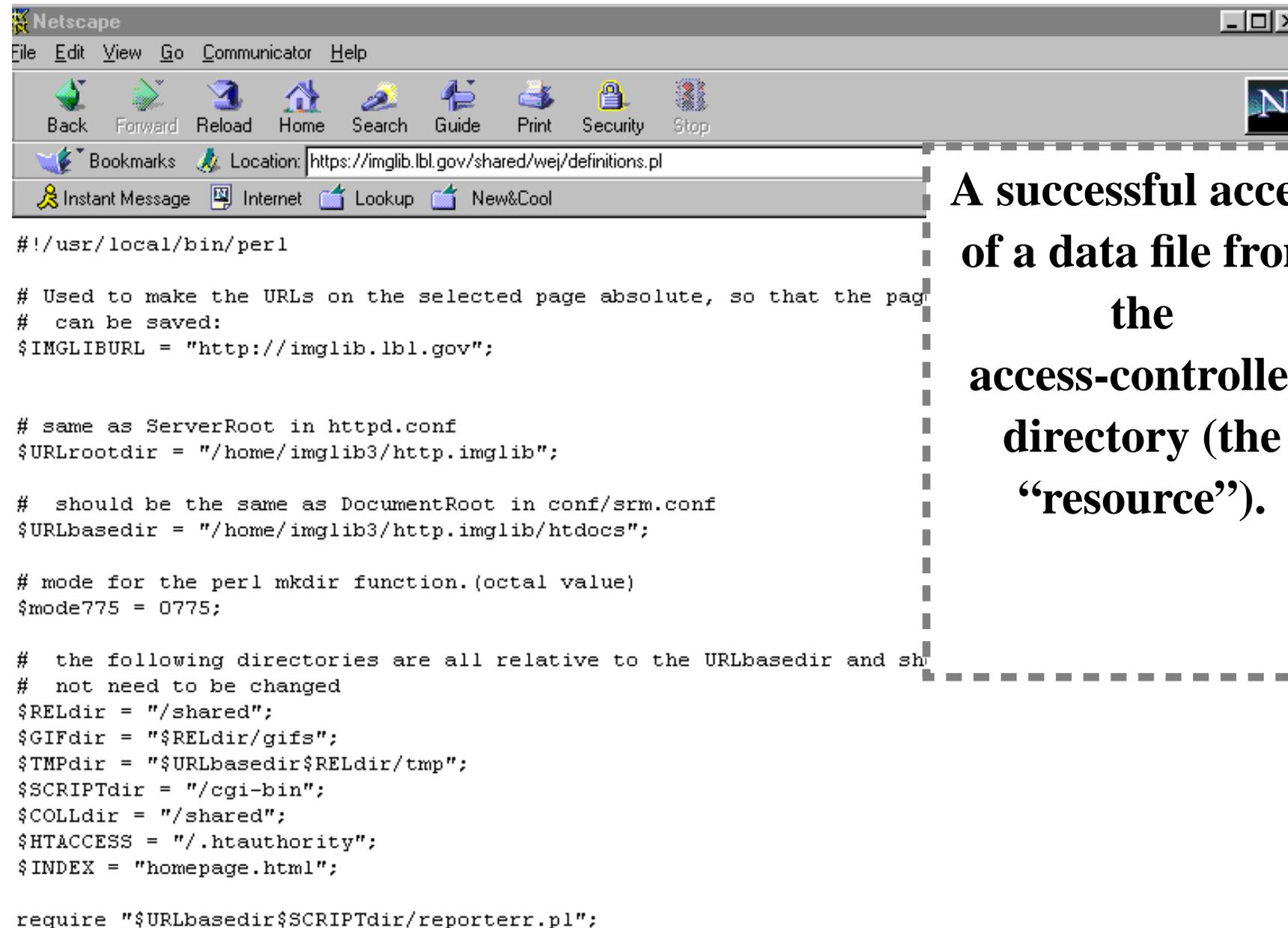
Index of /shared/wej

Name	Last modified	Size	Description
Parent Directory	16-Jan-98 16:42	-	
createdir.pl	17-Dec-97 19:07	4k	
definitions.pl	06-Jan-98 11:59	1k	
delete.cgi	06-Jan-98 12:00	2k	
fwwwhttp.pl	13-May-97 18:44	8k	
printenv	08-Sep-97 17:09	1k	
reporterr.pl	18-Dec-97 10:38	1k	
setup.cgi	16-Jan-98 16:00	4k	
storefile.cgi	06-Jan-98 12:00	8k	
wwdates.pl	13-May-97 18:44	8k	
wwwerror.pl	13-May-97 18:44	4k	
wwwmime.pl	13-May-97 18:44	4k	
wwwurl.pl	13-May-97 18:44	12k	

**Now the required
attribute
certificate is
available, and
access is allowed.**



Akenti: User Interaction



```
#!/usr/local/bin/perl

# Used to make the URLs on the selected page absolute, so that the page
# can be saved:
$IMGLIBURL = "http://imglib.lbl.gov";

# same as ServerRoot in httpd.conf
$URLrootdir = "/home/imglib3/http.imglib";

# should be the same as DocumentRoot in conf/srm.conf
$URLbasedir = "/home/imglib3/http.imglib/htdocs";

# mode for the perl mkdir function. (octal value)
$mode775 = 0775;

# the following directories are all relative to the URLbasedir and should
# not need to be changed
$RELDdir = "/shared";
$GIFdir = "$RELDdir/gifs";
$TMPdir = "$URLbasedir$RELDdir/tmp";
$SCRIPTdir = "/cgi-bin";
$COLLdir = "/shared";
$HTACCESS = "/.htauthority";
$INDEX = "homepage.html";

require "$URLbasedir$SCRIPTdir/reporterr.pl";
```

**A successful access
of a data file from
the
access-controlled
directory (the
“resource”).**



Akenti: User Interaction

