The Netscape Certification Authority: User Identity Establishment[1]

(As Used by the Akenti Access Control System)

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

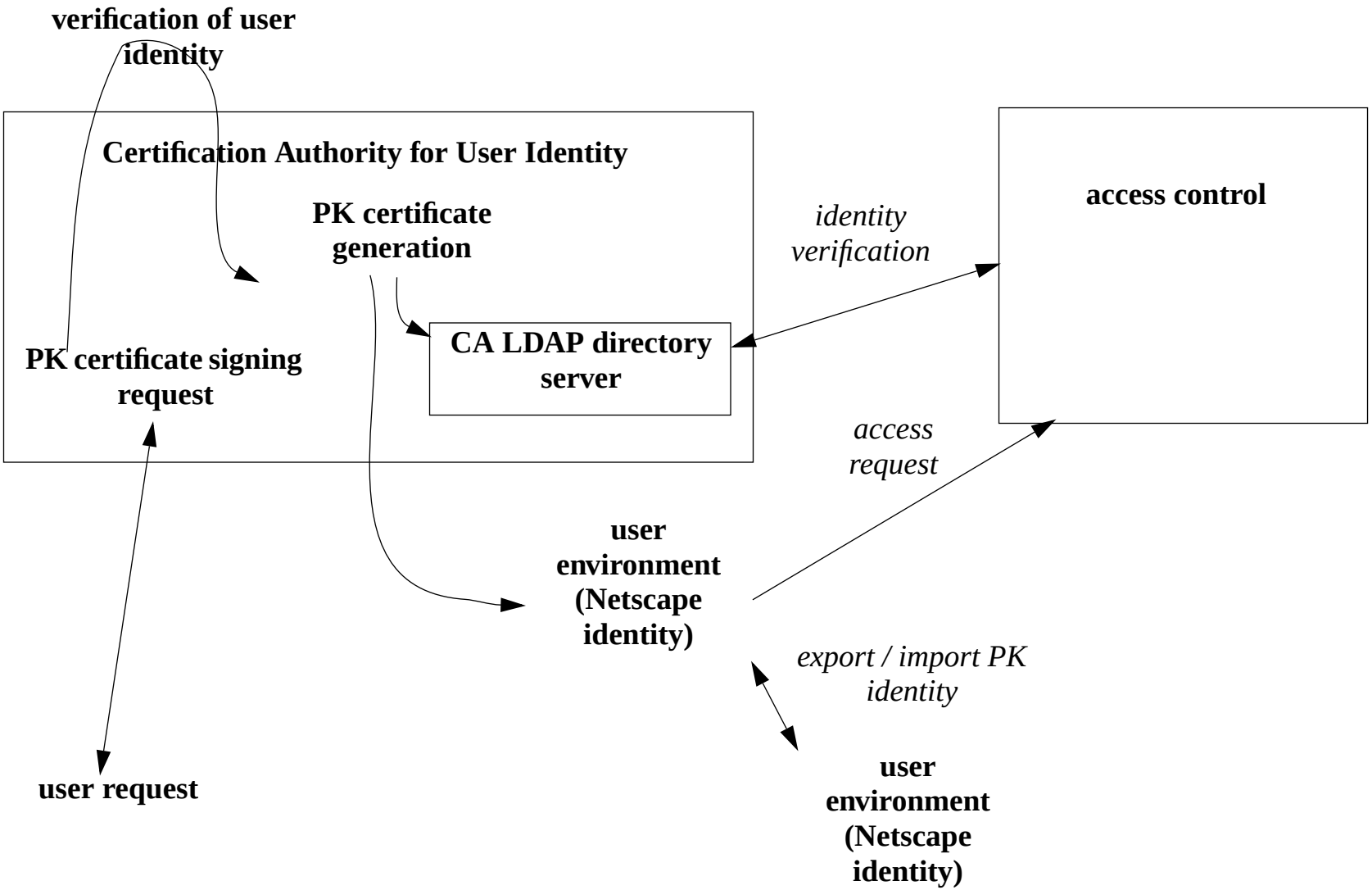
The Netscape CA - User Interaction

An identity certificate binds a user name to a public key in a document issued by a trusted third-party (the Certification Authority.) The private key and the public key are cryptographically bound - what one encrypts only the other can decrypt. It is this binding that allows the private key - if it has been held in confidence by its owner - to strongly authenticate the owner to anyone who obtains the owner's public key from the CA.

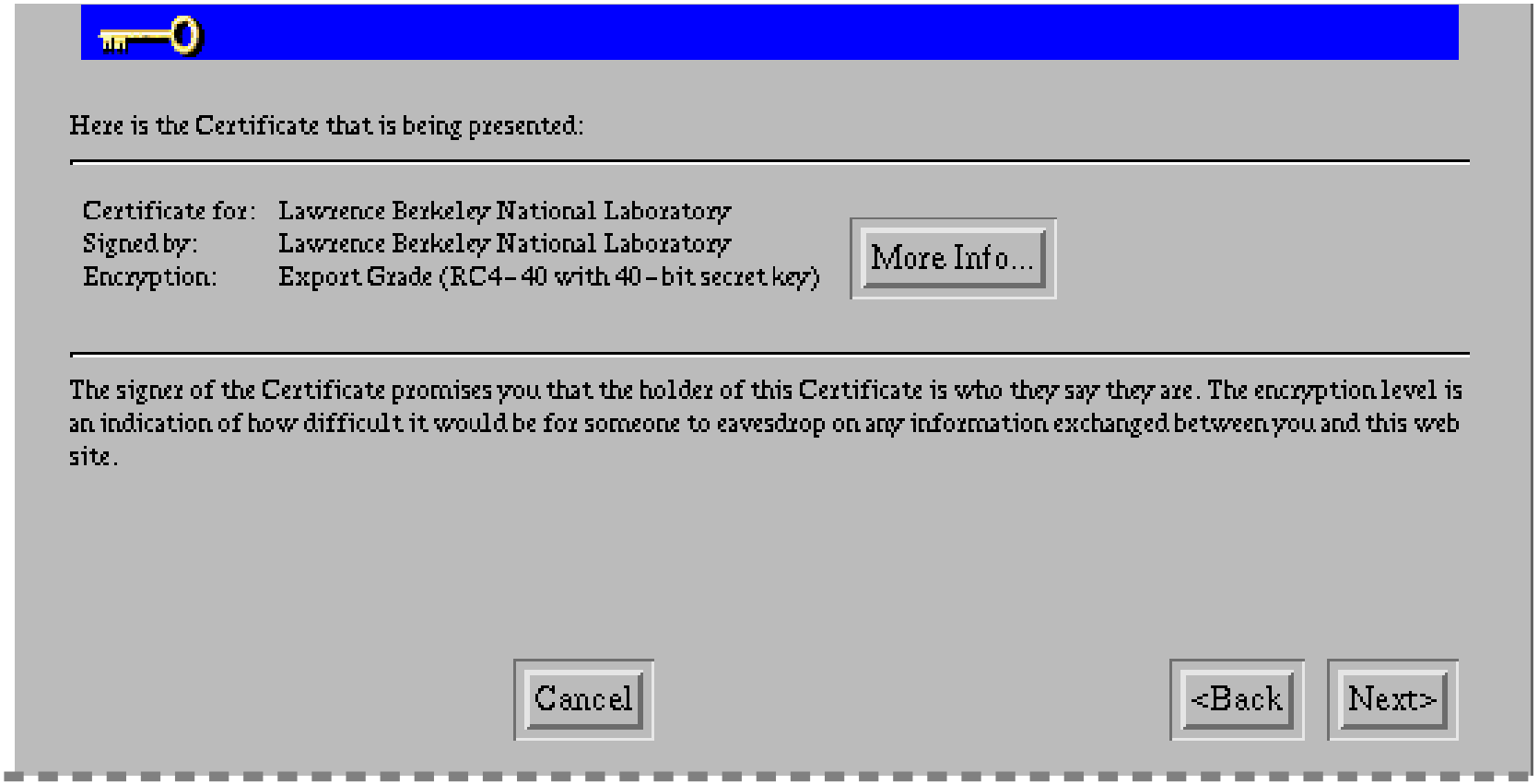
3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 21 22

Akenti / Netscape: Identity Establishment

Generation, Maintenance, and Use of A Public-Key Based Identity - Netscape CA



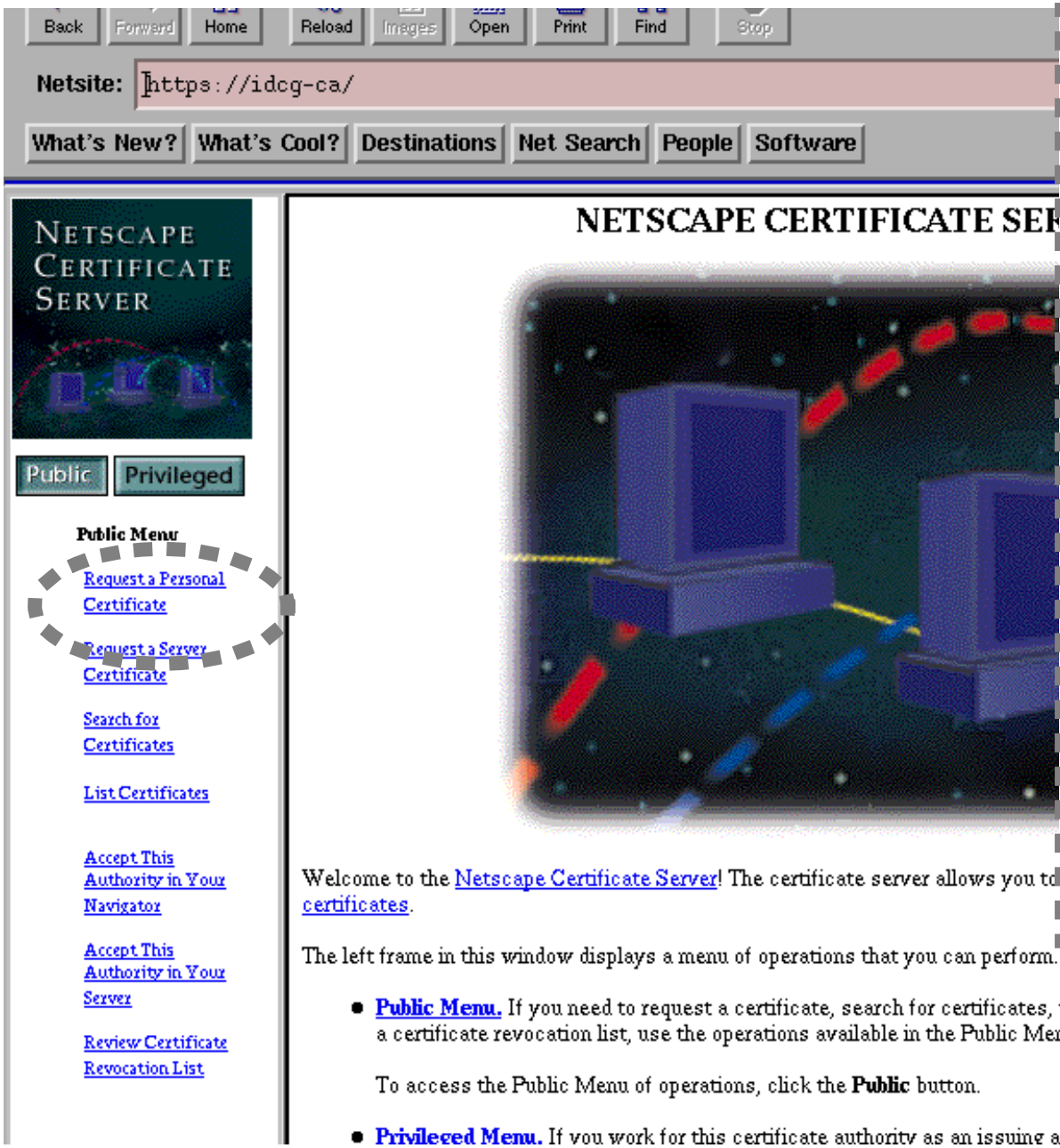
Akenti / Netscape: Identity Establishment



Accepting the CA's certificate.

The Netscape browser requires an explicit action on the part of the user if a certificate is presented to the browser.

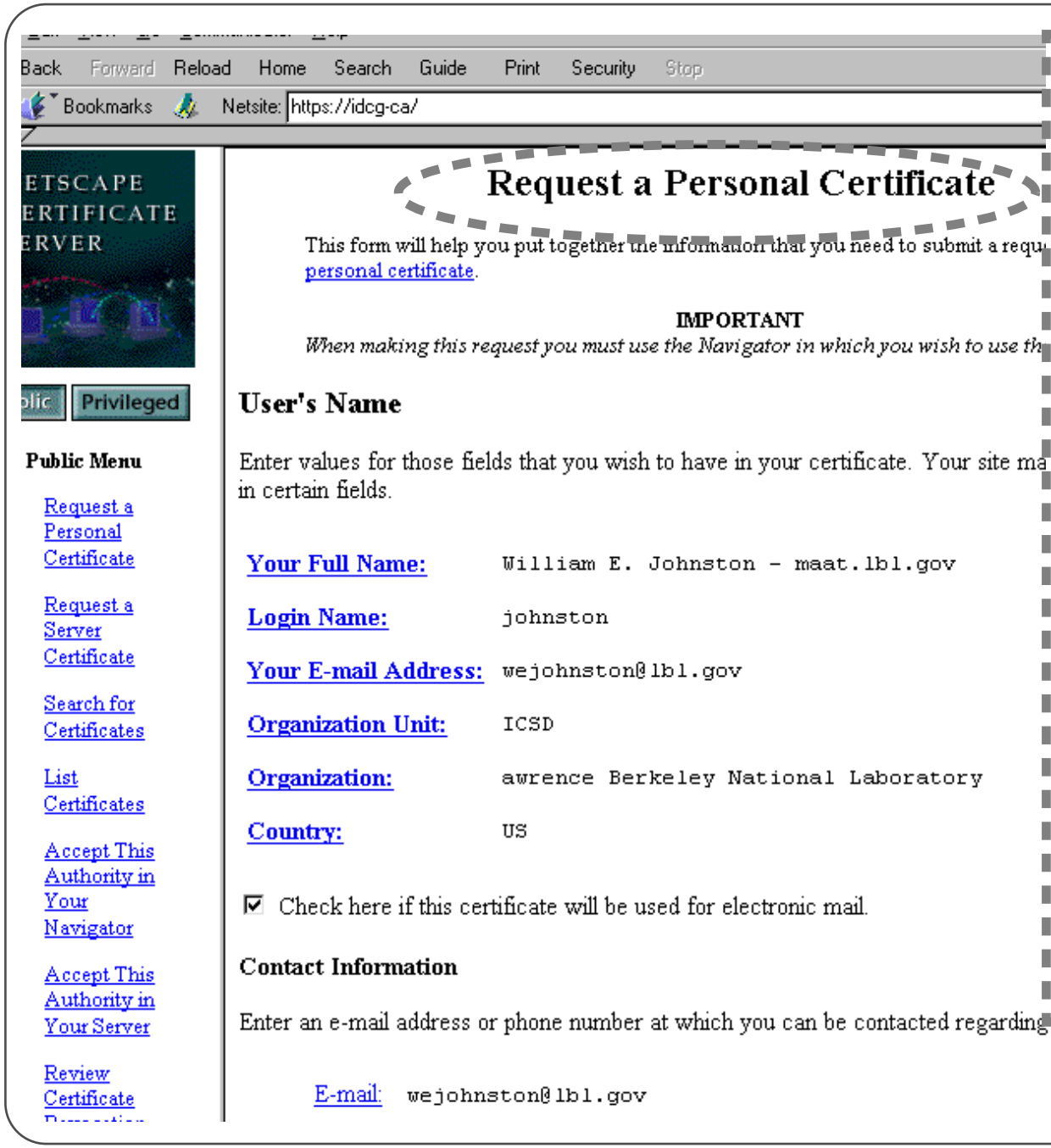
Akenti / Netscape: Identity Establishment



The Certification Authority issues identity certificates to users.

The CA will have a published policy on what is required of the user in order to receive a certificate. The request is received by the CA administrator and held until the user identity verification process has been completed.

Akenti / Netscape: Identity Establishment

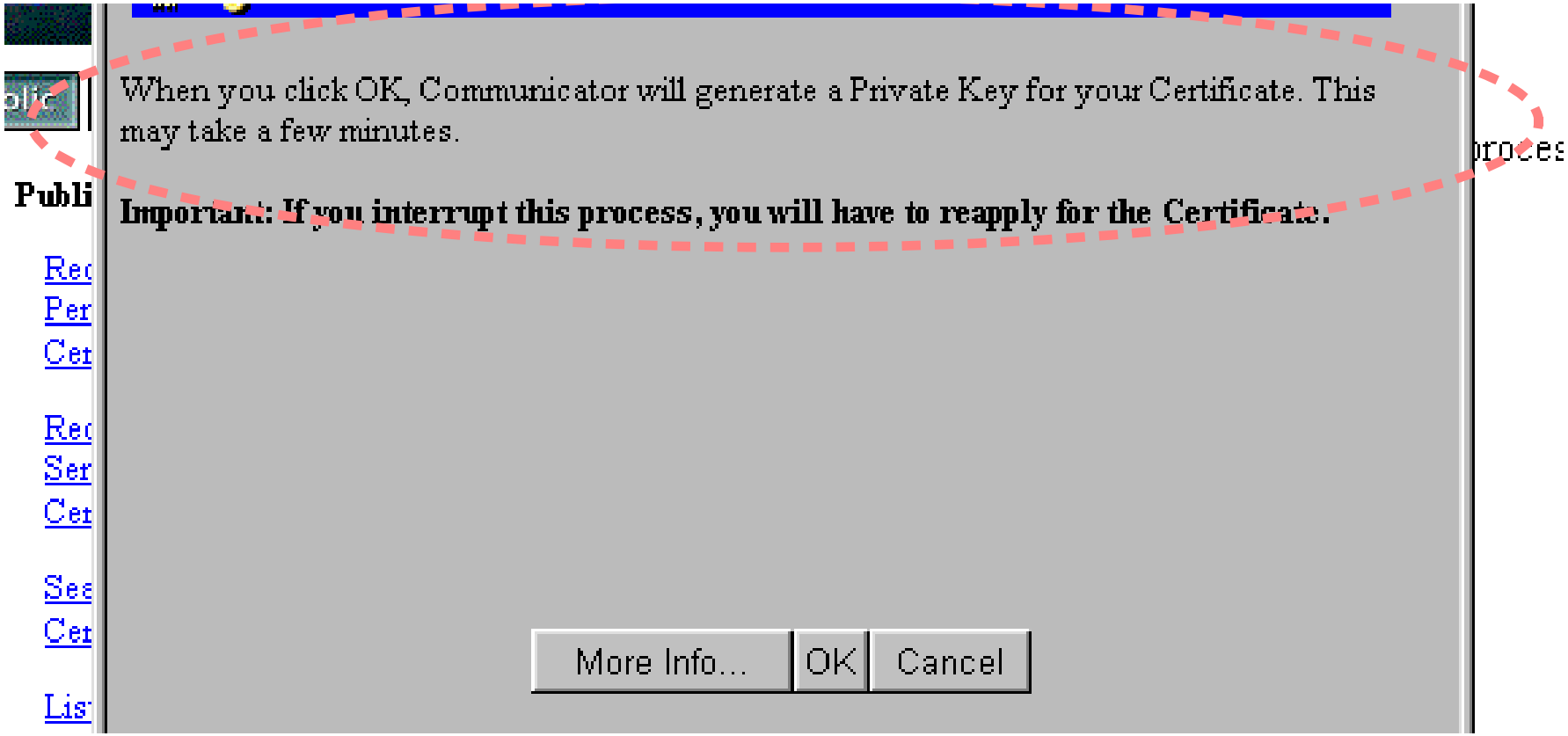


The user supplies the basic information for a certificate

"Your Full Name" becomes your "Common Name" in the X.509 certificate. If the same CA issues you multiple certificates, then the names must be unique.

The exact form of "Org. Unit", "Org.", and "Country" must be obtained from the CA

Akenti / Netscape: Identity Establishment



User key-pair generation

The browser generates you public/private key pair, stores the private key locally, and packages the public-key as part of the certificate request.

Akenti / Netscape: Identity Establishment

It is strongly recommended that you protect your Private Key with a Communicator password. If you do not want a password, leave the password field blank.

The safest passwords are at least 8 charaters long, include both letters and numbers, and contain no words from a dictionary.

Password: **********

Type it again to confirm: **********

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

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

Your private key IS your identity!!

Netscape keeps a database of private keys and the associated X.509 Common Names. This database must be passphrase protected. Use an unguessable, but easily remembered passphrase. WRITE IT DOWN (and carry it in your wallet or similarly private but convenient place).

Akenti / Netscape: Identity Establishment

Bookmarks Netsite: https://idcg-ca/

NETSCAPE CERTIFICATE SERVER

Public | Privileged

Public Menu

- Request a Personal Certificate
- Request a Server Certificate
- Search for Certificates
- List Certificates
- Accept This Authority in Your Navigator
- Accept This Authority in Your Server
- Review

Personal Certificate Signing Request

Your request has been submitted and will be processed by a representative of the certificate authority. Please include the reference number below when inquiring about this request. You should save this output until you receive the requested certificate.

Reference Number: 29

Subject Name

```
E=wejohnston@lbl.gov, CN=William E. Johnston - maat.lbl.gov, UID=johnston, OU=
```

Subject Public Key Information

```
Algorithm: PKCS #1 RSA Encryption
Public Key:
    Modulus:
        00:c5:8e:f4:83:a4:d7:84:86:9f:71:04:ed:94:df:90:c8:6c:d7:75:a8:62:83:
        d8:df:74:47:b3:39:be:20:ab:01:8b:23:08:b1:4e:73:59:ff:ae:52:b2:fc:85:
        5b:88:d1:06:52:cf:f9:4c:a2:d2:16:47:63:93:05:ac:fa:ec:bd
    Public Exponent: 65537 (0x10001)
```

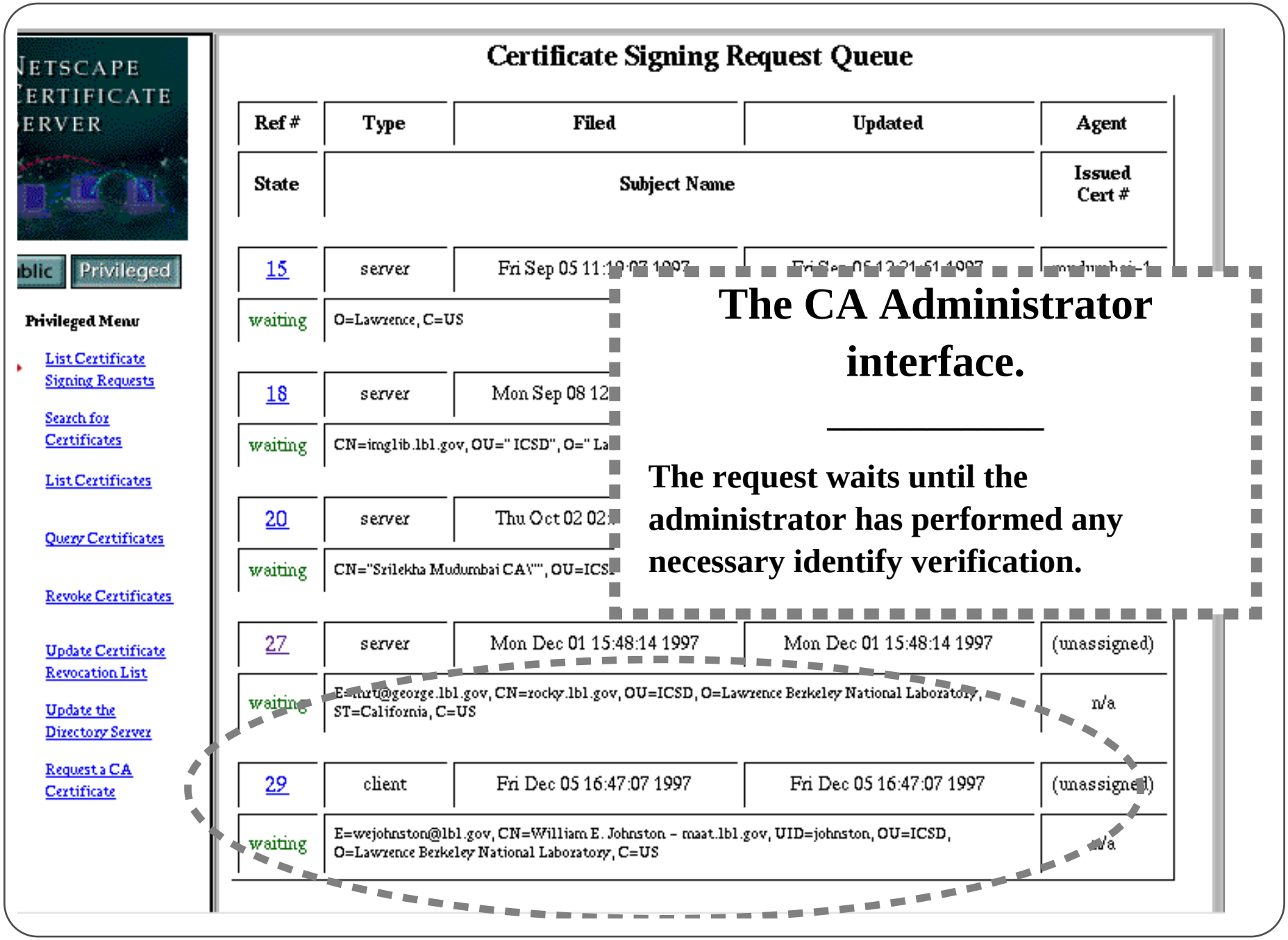
Requestor's Contact Information

Name: William E. Johnston - maat.lbl.gov

E-mail: wejohnston@lbl.gov

Phone: 510-486-5014

Akenti / Netscape: Identity Establishment



The CA Administrator interface.

The request waits until the administrator has performed any necessary identify verification.

Akenti / Netscape: Identity Establishment

note that their can be multiple certifiers

Privileged

ed Menu

Certificate
ing Requests

h for
ificates

Certificates

y Certificates

ke Certificates

ate Certificate
cation List

ate the
tory Server

est a CA
ificate

Status: waiting **Assigned To:** mudumbai

Requestor's Contact Information

Name: William E. Johnston – maat.lbl.gov
E-mail: wejohnston@lbl.gov
Phone: 510-486-5014

Desired Certificate Type: client

Subject Name

```
E=wejohnston@lbl.gov, CN=William E. Johnston - maat.lbl.gov, UID=johnsto
```

Subject Public Key Information

```
Algorithm: PKCS #1 RSA Encryption
Public Key:
    Modulus:
        00:c5:8e:f4:83:a4:d7:84:86:9f:71:04:ed:94:df:90:c8:6c:d7:75:a8:62:83:
        d8:df:74:47:b3:39:be:20:ab:01:8b:23:08:b1:4e:73:59:ff:ae:52:b2:fc:85:
        5b:88:d1:06:52:cf:f9:4c:a2:d2:16:47:63:93:05:ac:fa:ec:bd
    Public Exponent: 65537 (0x10001)
```

☐ Check to override public key uniqueness requirement

Length of Validity Period

6 Months (180 days)

☐ Check to override validity nesting requirement

Extensions

Netscape Certificate Type (Usage)

Enable for the following usage:

☐ SSL Client ☐ SSL Server ☐ Secure E-mail ☐ Object Signing

Key Identifiers

☐ Include Authority Key Identifier

☐ Include Subject Key Identifier

Reset To Original Request

Select Signature Algorithm:

MD5 With RSA Encryption

Select An Operation To Perform on This Request

Issue This Certificate

Perform Selected Operation | **Help**

y Certificates

ke Certificates

ate Certificate
cation List

ate the
tory Server

est a CA
ificate

Akenti / Netscape: Identity Establishment

File Edit View Go Bookmarks Options Directory Window Help

NETSCAPE CERTIFICATE SERVER

Public | Privileged

Privileged Menu

- List Certificate Signing Requests
- Search for Certificates
- List Certificates
- Query Certificates
- Revoke Certificates
- Update Certificate Revocation List
- Update the Directory Server
- Request a CA Certificate

Mail the completed certificate

Click here to mail the URL of the completed certificate request to the requestor.

The server issued the following certificate

```
Certificate:
    Data:
        Version: v3 (0x2)
        Serial Number: 28 (0x1c)
        Signature Algorithm: PKCS #1 MD5 With RSA Encryption
        Issuer: CN=IDCG-CA, OU=ICSD, O=Lawrence Berkeley National Laboratory, C=US
        Validity:
            Not Before: Fri Dec  5 16:56:38 1997
            Not  After: Wed Jun  3 17:56:38 1998
        Subject: E=wejohnston@lbl.gov, CN=William E. Johnston - maat.lbl.gov, UID=johnston, OU=ICSD
        Subject Public Key Info:
            Algorithm: PKCS #1 RSA Encryption
            Public Key:
                Modulus:
                    00:c5:8e:f4:83:a4:d7:84:86:9f:71:04:ed:94:df:90:c8:6c:
                    d7:75:a8:62:83:d8:df:74:47:b3:39:be:20:ab:01:8b:23:08:
                    b1:4e:73:59:ff:ae:52:b2:fc:85:5b:88:d1:06:52:cf:f9:4c:
                    a2:d2:16:47:63:93:05:ac:fa:ec:bd
                Public Exponent: 65537 (0x10001)
        Extensions:
            Identifier: Certificate Type
                Critical: no
                Certified Usage:
                    SSL Client
                    Secure E-mail
            Identifier: Authority Key Identifier
                Critical: no
                Key Identifier:
                    09:07:1d:ab:52:ef:c1:5a:6b:33:b9:0b:94:f2:e5:ed:f9:96:
                    e0:fb
    Signature:
        Algorithm: PKCS #1 MD5 With RSA Encryption
        Signature:
            84:c2:2c:20:bd:1f:59:9f:05:d1:93:29:f6:69:94:a6:68:eb:a2:12:b4:
            2c:e5:44:42:2d:e5:01:81:ba:18:9a:64:73:57:88:e5:46:43:00:f4:9b:
            6a:1a:54:4c:21:9d:22:c4:52:9b:8f:1e:e9:a3:5f:46:1a:27:3b:fd:e9:
            f6:24:38:61:d2:01:a8:bc:06:1e:78:96:8a:e8:ba:17:c1:b7:40:b0:aa:
            c2:5f:3f:28:7e:f3:40:c1:44:fc:7f:aa:96:3d:c5:e3:57:8f:c1:d6:d4:
            43:92:dc:f2:87:be:38:68:fc:e8:2d:a2:72:06:d6:de:d8:4c:1e:6c:6d:
            80:2a
```

Requestor's Contact Information

Name: William E. Johnston – maat.lbl.gov
E-mail: wejohnston@lbl.gov
Phone: 510-486-5014

Installing This Certificate In a Server

The following format can be used to install this certificate into a Netscape server using the server's administration forms under the menu bar category *Encryption*.


```
-----BEGIN CERTIFICATE-----
MIICfTCCAeagAwIBAgIBHDANBgkqhkiG9w0BAQQFADBeMQswCQYDVQQGEwJVUzEu
MCwGA1UEChMlTGF3cmVuY2UgQmVya2VsZXkgTmF0aW9uYWwgTGFib3Jhdd9yeTEN
MAsGA1UECxMESUNTRDEQMA4GA1UEAxMHSURDRy1DQTAeFw05NzEyMDYwMDU2Mzha
Fw050DA2MDQwMDU2MzhaMIG2MQswCQYDVQQGEwJVUzEuMCwGA1UEChMlTGF3cmVu
Y2UgQmVya2VsZXkgTmF0aW9uYWwgTGFib3Jhdd9yeTENMAsGA1UECxMESUNTRDEY
MBYGCgmSJomT8ixkAQETCGpvaG5zdG9uMSswKQYDVQQDEyJXaWxsaWFtIEUuIEpv
aG5zdG9uIC0gbWFhdc5sYmwuZ292MSEwHwYJKoZIhvcNAQkBFhJ3ZWpvaG5zdG9u
QGxibC5nb3YwXDANBgkqhkiG9w0BAQEFAANLADBIAkEAxY70g6TXhIafcQTtlN+Q
yGzXdahig9jfdEezOb4gqwGLIwixTnNZ/65SsvyFW4jRBlLP+Uyi0hZHY5MFrPrs
vQIDAQABozYwNDARBglghkgBhvhCAQEEBAMCAKAwHwYDVR0jBBgwFoAUCQcdqlLv
wVprM7kLlPL17fmW4PswDQYJKoZIhvcNAQEEBQADgYEAhMIsIL0fWZ8F0Zmp9mmU
pmjrohK0L0VEQi3lAYG66Jpkc1eI5UZDAPSbahpUTCGdIsRSm48e6aNfRhon0/3p
9iQ4YdIBqLwGHniWiui6F8G3QLCqwl8/KM7zQMFE/H+qlj3F41ePwdbVQ5Lc8oe+
0Gj86C2icgbW3thMHmxtgCo=
-----END CERTIFICATE-----
```


Importing This Certificate To a Navigator

If this certificate is for your personal use, you can click on this link now or open this location later

https://idcg-ca.lbl.gov/cms?op=getBySerial&serialNumber=1c

In order to import this certificate into your Navigator's list of Personal Certificates. If this certificate is for use by another user or by a server, you can forward this page to that user or to the server's administrator to facilitate installation.

Directory Update Result

Note: The new certificate could not be published in the directory.
Error returned: Could not find a matching entry in the directory.

This representation of, and pointer to, the certificate is mailed to the user.

Akenti / Netscape: Identity Establishment

Personal Certificate Signing Request

Your request has been submitted and will be processed by a representative of the certificate authority. Please include the reference number below when inquiring about this request. You should save this output until you receive the requested certificate.

Reference Number: 29

Subject Name

E=wejohnston@lbl.gov, CN

Subject Public Key Informati

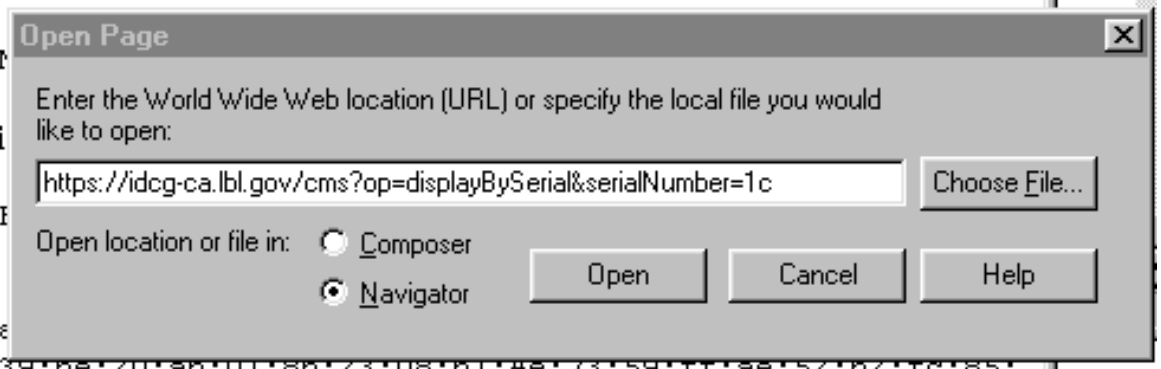
```
Algorithm: PKCS #1 RSA E
Public Key:
    Modulus:
        00:c5:8e:f4:83:e
        d8:df:74:47:b3:39:be:20:ab:01:8b:23:08:b1:4e:73:59:11:ae:52:b2:1c:85:
        5b:88:d1:06:52:cf:f9:4c:a2:d2
    Public Exponent: 65537 (0x10001)
```

Requestor's Contact Information

Name: William E. Johnston - maat.lbl.gov

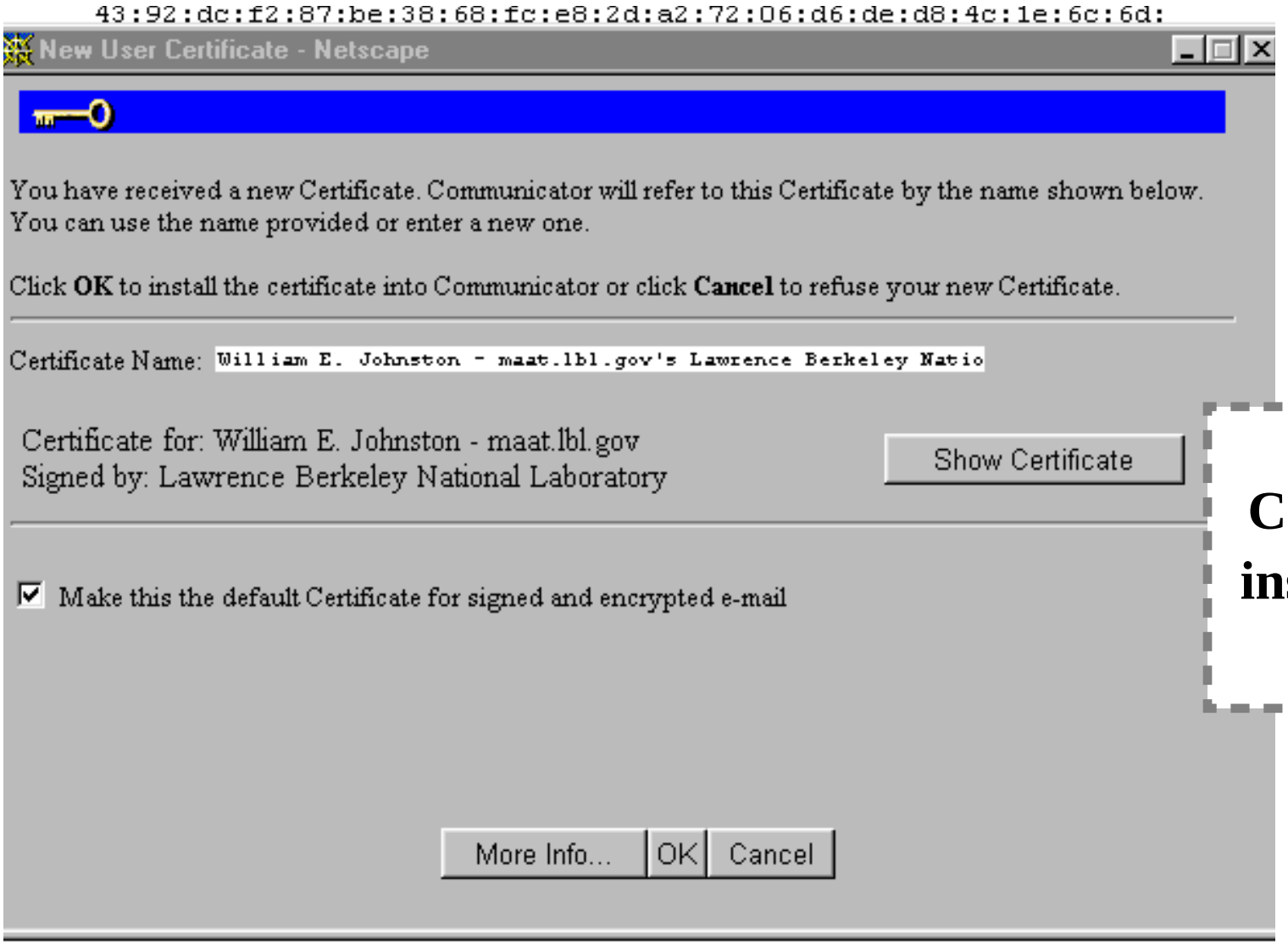
E-mail: wejohnston@lbl.gov

Phone: 510-486-5014



The certificate pointer that was mailed by the CA is invoked by the user to install the certificate in the local environment.

Akenti / Netscape: Identity Establishment

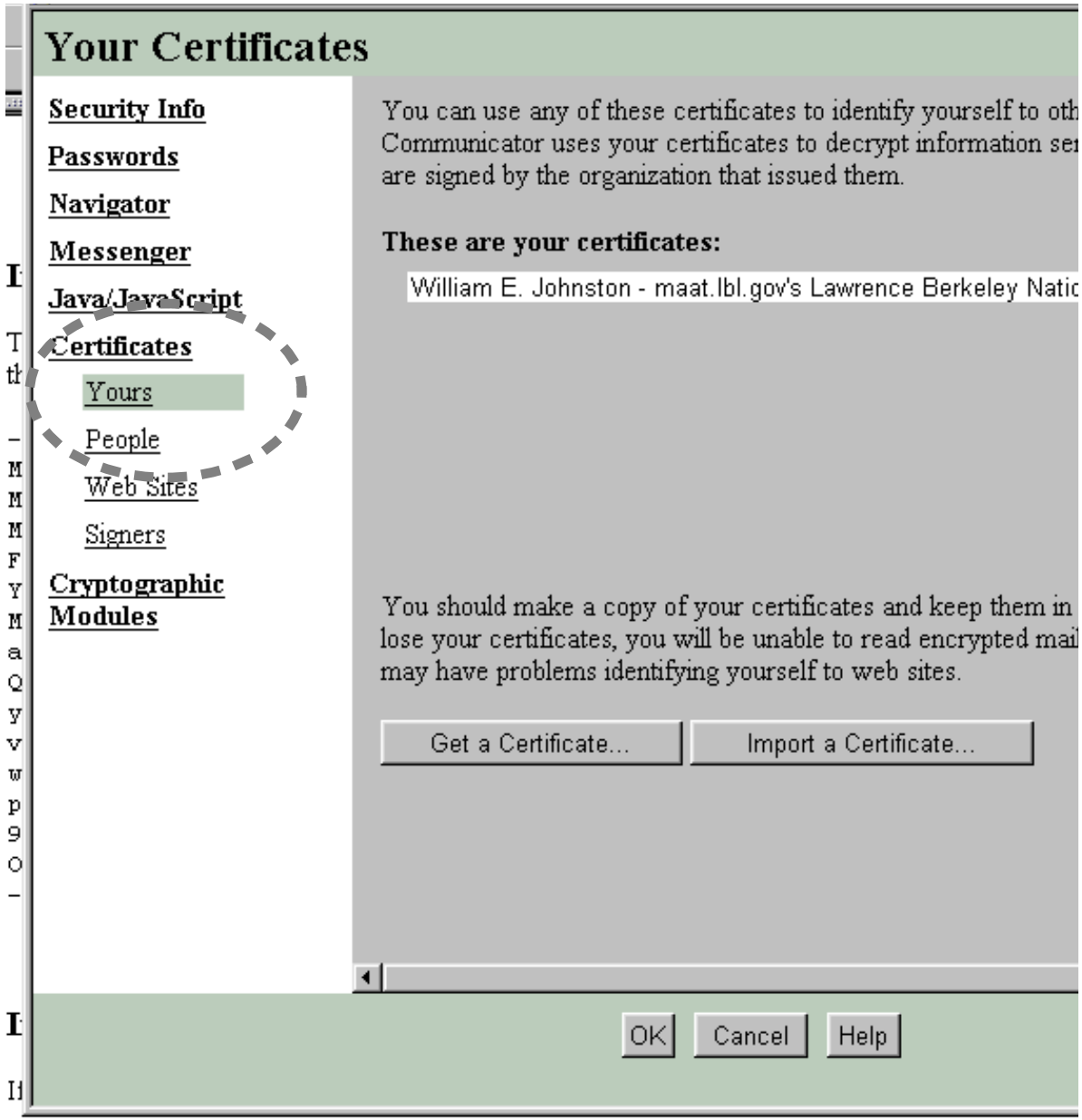


Certificate installation

This Certificate To a Navigator

te is for your personal use, you can click on this link now or open this location later

Akenti / Netscape: Identity Establishment



https://idcg-ca.lbl.gov/cms?op=getBySerial&serialNumber=1c

The Netscape 4 / Communicator Security interface - after the new certificate has been installed.

Akenti / Netscape: Identity Establishment

The CA Administrator contacts the directory server to install the new User Certificate in the CA LDAP database so that it will be available to Akenti.

Akenti / Netscape: Identity Establishment

Netscape: Netscape Directory Server Gateway

File Edit View Go Bookmarks Options Directory Window

Netscape Directory Server™ 1.01

© 1996 Netscape Communications Corporation. All Rights Reserved.

Smart Search | Advanced Search | New Entry | Authentication

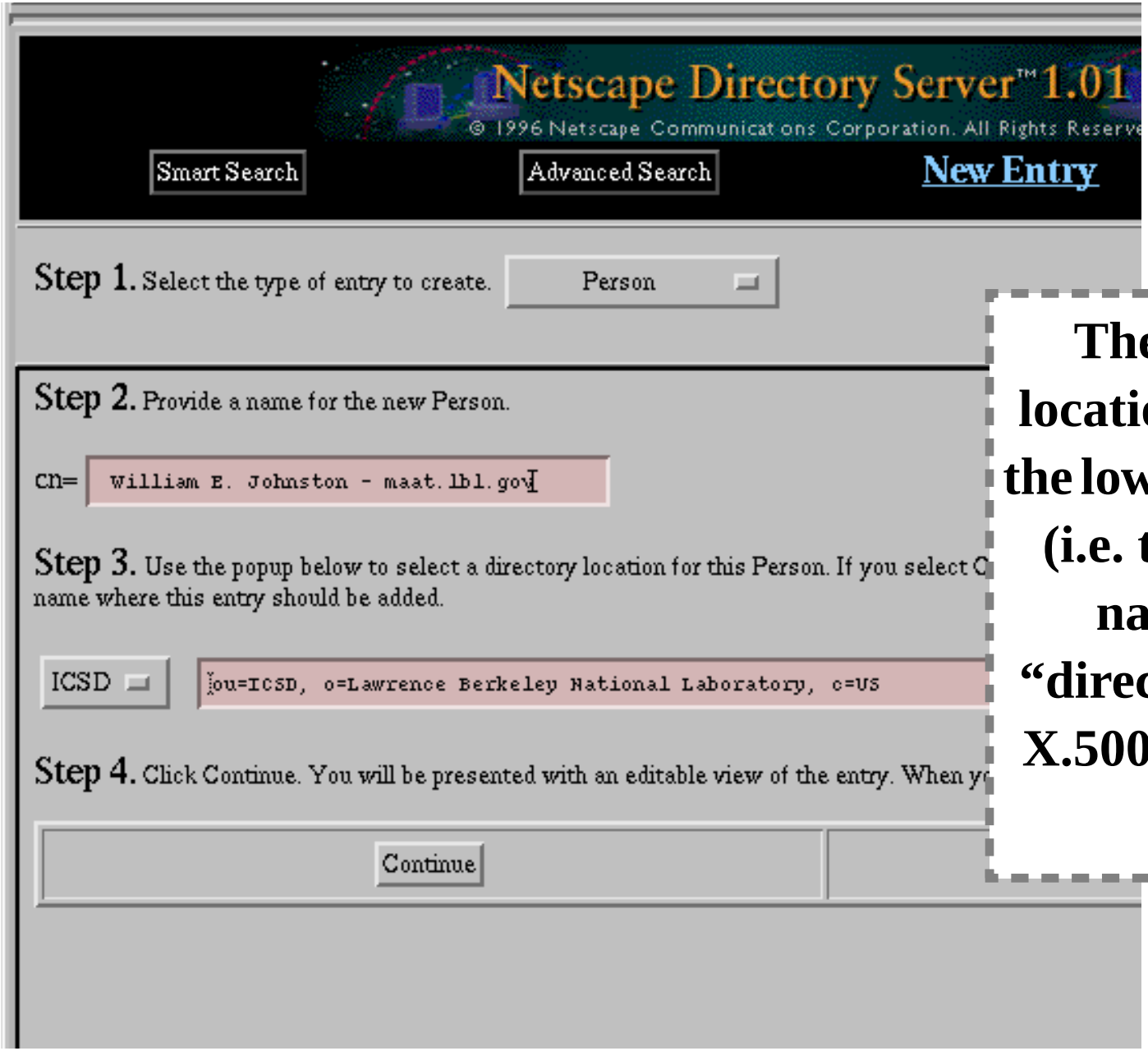
Welcome to the Netscape Directory Server Gateway

With the Netscape Directory Server Gateway, you can search for, modify, and create entries in the Netscape Directory Server.

The toolbar you see at the top of this window is always available when you are using the Directory Server Gateway. You can click on the b
perform any of the following tasks:

Smart Search	Smart search is the easiest way to search the directory. Smart search examines what you type and automatically sele more methods of searching the directory.
Advanced Search	With Advanced Search, you can specify exactly what you are looking for, what attribute you wish to search for, and w of matching you wish to allow.
New Entry	New Entry allows you to create new entries in the directory. Depending on how the system administrator has set up y directory, you may need to be granted special permission to add new entries. If you are not sure, ask your system adm
Authenticate	You use the authentication screens to log into and out of the directory. You need to authenticate before you can modi entries to the directory. You may also need to authenticate before searching the directory, if your system administrat it.

Akenti / Netscape: Identity Establishment



The directory location is given as the lowest level node (i.e. the full path name of the "directory") in the X.500 information tree.

Akenti / Netscape: Identity Establishment

Back Forward Home Reload Images Open Print Find Stop

Location: http://idcg-ds.lbl.gov/ds/edit/cn%3DWilliam%20E.%20Johnston%20-%20maat.lbl.gov%2C%20ou%

What's New? What's Cool? Destinations Net Search People Software

* Indicates a required field

First Name:

Full Name: * William E

Last Name: * Johnston

Password:

Repeat password to confirm:

Phone:

E-Mail Address:

Fax:

User ID:

Pager:

Mobile Phone:

Business Category:

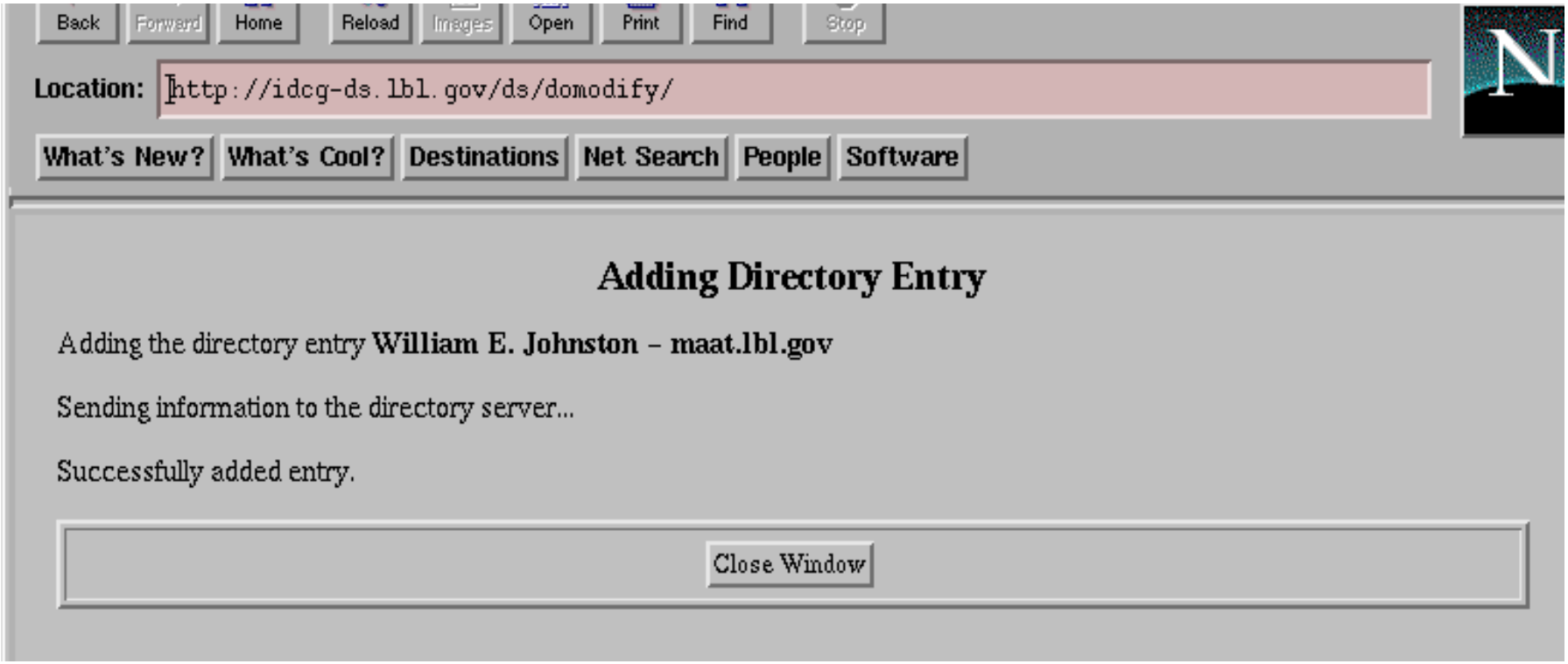
Title: user

Organizational

Manager:

The directory can probably be populated automatically with associated information.

Akenti / Netscape: Identity Establishment



Identity certificates must be in the CA's LDAP server for Akenti to be able to use them.

Akenti / Netscape: Identity Establishment

leged

enu

icate
quests

s

icates

ificates

tificates

tificate
List

erver

A

Update the Directory Server

In most cases, the directory is updated automatically with the latest changes to certificates and certificate revocation lists. In a few situations, however, you may need to update the directory manually. In those cases, you can use this form to make any necessary updates manually.

Note: Any certificates issued or revoked during the update may or may not be reflected in the directory. You may use this form again to update those certificates.

Check one or more boxes below.

- ☐ **Update everything in the database to the directory.**
  (This will include all selections below.)
- ☐ **Update the certificate revocation list to the directory.**
- ☐ **Update valid certificates to the directory.**
  - From Serial Number: [ ] (blank for no lower limit)
  - To Serial Number: [ ] (blank for no upper limit)
- ☐ **Remove expired certificates from the directory.**
  - From Serial Number: [ ] (blank for no lower limit)
  - To Serial Number: [ ] (blank for no upper limit)
- ☐ **Remove revoked certificates from the directory.**

Directory server maintenance.

Akenti / Netscape: Identity Establishment

```
 144 cert7.db                          0 preferences.js
   6 cookies                           2 registry
 304 history.db                       48 secmodule.db
   2 history.list
mudumbai@portnoy(7)>netscape&
[1] 16237
mudumbai@portnoy(8)>ldapsearch -b "cn=William E. Johnston - maat.lbl.gov,ou=ICSD
,o=Lawrence Berkeley National Laboratory,c=US" -h idcg-ds.lbl.gov "cn=*"
cn=William E. Johnston - maat.lbl.gov, ou=ICSD, o=Lawrence Berkeley National Lab
oratory, c=US
objectclass=top
objectclass=person
objectclass=organizationalPerson
objectclass=inetOrgPerson
cn=William E. Johnston - maat.lbl.gov
sn=Johnston
title=user
creatorsname=cn=Directory Manager,o=Lawrence Berkeley National Laboratory,c=US
createtimestamp=19971206011959Z
modifytimestamp=19971206012107Z
modifiersname=cn=Directory Manager,o=Lawrence Berkeley National Laboratory,c=US
usercertificate;binary:: MIICfTCCAeagAwIBAgIBHDANBgkqhkiG9w0BAQQFADBeMQswCQYD
 VQQGEwJVUzEuMCwGA1UEChM1TGF3cmVuY2UgQmVya2VsZXkgTmF0aW9uYWwgTGFib3JhdG9yeTEN
 MAsGA1UECxMESUNTRDEQMA4GA1UEAxMHSURDRylDQTAeFw05NzEyMDYwMDU2MzhaFw050DA2MDQw
 MDU2MzhaMIG2MQswCQYDVQQGEwJVUzEuMCwGA1UEChM1TGF3cmVuY2UgQmVya2VsZXkgTmF0aW9u
 YWwgTGFib3JhdG9yeTENMAsGA1UECxMESUNTRDEYMBYGCgmSJomT8ixkAQETCGpvaG5zdG9uMSsw
 KQYDVQQDEyJXaWxsaWFtIEUuIEpvaG5zdG9uIC0gbWFhdC5sYmwuZ292MSEwHwYJKoZIhvcNAQkB
 FhJ3ZWpvaG5zdG9uQGxibC5nb3YwXDANBgkqhkiG9w0BAQEFAANLADBIAkEAxY70g6TXhIafcQTt
 lN+QyGzXdahig9jfdEez0b4gqwGLIwixTnNZ/65SsvyFW4jRB1LP+Uyi0hZHY5MFrPrsvQIDAQAB
 ozYwNDARBglghkgBhvhCAQEEBAMCAKAwHwYDVR0jBBgwFoAUCQcdqlLvwVprM7kL1PL17fmW4Psw
 DQYJKoZIhvcNAQEEBQADgYEAhMIsIL0fWZ8F0ZMp9mmUpmjrohK0L0VEQi31AYG6GJpkcleI5UZD
 APSbahpUTCGdIsRSm48e6aNfRhon0/3p9iQ4YdIBqLwGHniWiui6F8G3QLCqw18/KH7zQMFE/H+q
 lj3F41ePwdbUQ5Lc8oe+0Gj86C2icgbW3thMHmxtgCo=
mudumbai@portnoy(9)>
mudumbai@portnoy(9)>
```

manual LDAP query to check the installation of the new certificate

response