MMC Certificate Infrastructure

James A. Rome, Oak Ridge National Laboratory
jar@ornl.gov

May, 1999

Introduction

We all agree on the need for security. However, there are many ways to achieve different levels of security. The purpose of this paper is to outline the needs of the MMC, to explain how certificates meet these needs, and to guide you through the certificate issuing and use process.

Contents

Why are certificates the best MMC security solution?

What are the threats?

The threats to security are well known, but I reiterate them here because it is necessary to keep them in mind when proposing a security solution.

- Confidentiality – Protection of information from disclosure to unauthorized entities
- Integrity – Prevention of unauthorized changes to information
- Availability – Ability to access a resource whenever needed
- Authenticity – Confidence that a message was sent by a certain party and not an impostor

Because we work for the government, we are also subject to other restrictions and guidelines that loosely fall under the security banner:

- Prevention of the use government facilities for unauthorized activities
- Maintenance of audit trail
- Protection against the spread of malicious code (viruses, worms,...)

For example, we do not want any of our computers to serve as distribution points for games or pornography, nor do we want supporters of Kevin Mitnyck to hack our sites and claim that they have planted a new time bomb in our visitor's computers.

MMC issues

I feel strongly that as a collaboratory, we should make every effort to create a unified security solution that is strong enough to protect, but that is flexible enough to meet our differing security requirements. I list a few of the requirements for a good security solution:

flexibility
The security system should be able to protect all of our resources as well as implementing security policies that are more sophisticated than mere file-access restrictions.

user friendliness
Using a system with good security should be at last as easy as using one without security.

Scalability
Solutions should scale well as more facilities or users are added to the MMC.

Uniformity
The solutions should look the same (but may have differing properties) across the MMC.

Collaborating
Things that encourage the collaboratory aspects of the MMC should be encouraged.

Cutting edge, not bleeding edge = Pizzazz
We are a demo project, leading the way towards the future. We need to be implementing the solutions of the future even though they may cause us some short-term difficulties.

Certificates — now and in the future

The security field is evolving rapidly, and new solutions, problems, and tools appear daily. Our task is to try to predict the future course of events and to pick the winning solution. Since the MMC was launched last Spring, all events have served to confirm our initial choice of using certificates as the basis for MMC security. Like it or not, certificates will soon be a part of everyone's electronic persona

Identity certificates

Currently there are three certificates involved in each secure Web transaction.
- Server certificate: Attests to the identity of the Web server owner.
- Client certificate: Attests to the identity of the Web user (customer).
- Certificate authority certificate: Attests to the identity of the certificate authority (CA) that signed the server and client certificates.

In principal, there is a root CA certificate that is self signed and that everyone trusts. If the root CA certificate is compromised, the whole certificate structure falls apart. Thus, the private key for the SET (secure electronic transaction) infrastructure developed by Visa, MasterCard and American Express is split up into about a dozen electronic tokens dispersed throughout the world. The token holders meet once a year, but only a subset of them is required to transact business. For the MMC, less Draconian measures are called for. I am the root CA and have self signed the MMC CA certificate (in the name of the MMC). Due care is taken to keep the CA machine backed up and locked up in a secure location. This is the correct thing to do because for our purposes, we trust ourselves more than we trust an external CA such as VeriSign.

The format for identity certificates is spelled out in the PKI (public key infrastructure) specifications called X.509. Currently, the certificates we issue correspond to the latest, version 3 specification. These certificates bind an identity in the real world to a public key. For our purposes, our unique identity is specified by what is called a distinguished name (DN) which is composed of a person's real name, country, organization, city, and e-mail address. However, since certificates can also be issued to computers and other non-human entities, the notion of an identity is actually broader and fuzzier than might be ideal. An X.509v3 certificate allows a user to create a digital signature, to use the keys for encryption, to create S/MIME e-mail, and to sign trusted objects (e.g., Active-X controls). These privileges are actually delegated separately by different bits in the certificate's extensions. The contents of my MMC certificate show that I can use my certificate as an SSL client, for secure E-mail, and for object signing.

It is perhaps a philosophical issue, but the original goal of a certificate authority hierarchy, which would allow each certificate to be traced up to the root CA, was never established because the notion of an identity does not scale well. In a small community, everyone knows everyone else so the binding of a name to an identity is not difficult. However, if your friend John Smith moved to New York City, it will be very difficult to know which John Smith in the telephone book is your friend. Fortunately, the MMC community is small, so we can be confident

(enough?) of the identity of our users.

Uses of identity certificates

Once you have an identity certificate, what good is it? Until recently, X.509 certificates didn't even make good wall paper. However, the situation has changed dramatically with the introduction of Netscape 4.0. I will go over the things you can do with a certificate today and explain why this is an advance.

Secure Web access

Identity certificates allow user-friendly, secure access to a Web site with strong authentication. Modern Web servers (Netscape, IIS, Apache-SSL) can all be set up to require client certificates for site access. Out of the box, it is trivial to configure the server to accept only MMC certificates, so that anyone with a valid MMC certificate will be authenticated securely and can use SSL for secure access. No user ids and passwords are required. However, once per Netscape session, the user will have to unlock his private certificate key with a local password. The ORNL secure web site is set up this way on a Netscape Enterprise Server. To access this server, go to https://mmc.cind.ornl.gov/enote.

Access to a site can also be controlled by using "basic" authentication — user ids and passwords. There are several problems with this approach. The biggest problem is that this solution does not scale well. For example, at ORNL the MMC has at least six Web servers. If a new user is added and we used basic authentication, we would have to enroll the user separately at each server. Then there is the problem of allowing the user to securely set his password on each of these machines, especially if you do not want to give the user a login account of the machine (an invitation to a security breach). With MMC issued certificates, new users are automatically granted access to all MMC sites requiring certificates for access. Finally, there is generally no restriction to the number of times that a password-based Web access pop up can fail (or else there could be easy denial of service attacks). Therefore, access via user id and password is subject to password guessing attacks.

Digital signatures

Client certificates allow users to sign things, solving the *authenticity* security requirement. It is very easy to spoof E-mail, so it is good practice to sign all electronic communications. The PGP community has been routinely signing all their mail for years, but I feel that the X.509 solution is better and more user friendly than PGP.

PGP uses identity certificates also. However, PGP certificates are not signed by a CA. They are signed by your friends and acquaintances, or other people who vouch for your identity. This is called the "web of trust" model. X.509 certificates are signed by a CA that presumably you trust. There is much less baggage associated with X.509 because you do not have to go to key signing parties to get your PGP key well validated.

Yes, I know that not everything needs to be signed, but sending signed mail allows the recipients to obtain your public key so they can send encrypted mail back to you. Disk space is cheap. If you read the mail with the Netscape mail agent, the signature is reduced to an icon on the page rather than a lot of characters. It is a nuisance to turn signatures on and off as needed. Our goal is to make it easier for people.

Cyber identity

Your public key is your cyber identity. It can be used in other contexts to grant you authority to do things. The concept of authority certificates is the basis for the SPKI (simple public key infrastructure) that is currently in an IETF draft. See http://www.clark.net/pub/cme/html/spki.html. Provided that you can access your private key to unlock your certificate (to prevent spoofing), extremely complicated security policies can be implemented using a collection of authorization certificates.

S/MIME e-mail

S/MIME is a specification for secure electronic messaging. In 1995, several software vendors got together and created S/MIME to solve a very real problem - interception and forgery of e-mail. Protecting sensitive data is a real concern, especially in a world that is becoming increasingly more wired. The goal of S/MIME is to make it easy to secure messages from prying eyes. Since its creation, S/MIME has come a long way. Netscape and Microsoft's Outlook Express both support S/MIME encrypted and signed e-mail. Eudora Pro (PC only) supports the WorldSecure S/MIME plug-in. All of the major industry players have also agreed to support the S/MIME standard. A detailed list of S/MIME participants and computability testing results are available at http://www.rsa.com/smime/html/interop_center.html.

Again, sending secure e-mail is like practicing safe sex — you need to do it. Yes, not everything you send needs to be encrypted. However, it is very easy to intercept e-mail and to modify it. A malicious entity can put damaging words into your innocent e-mail. In today's world, security by obscurity does not work any more.

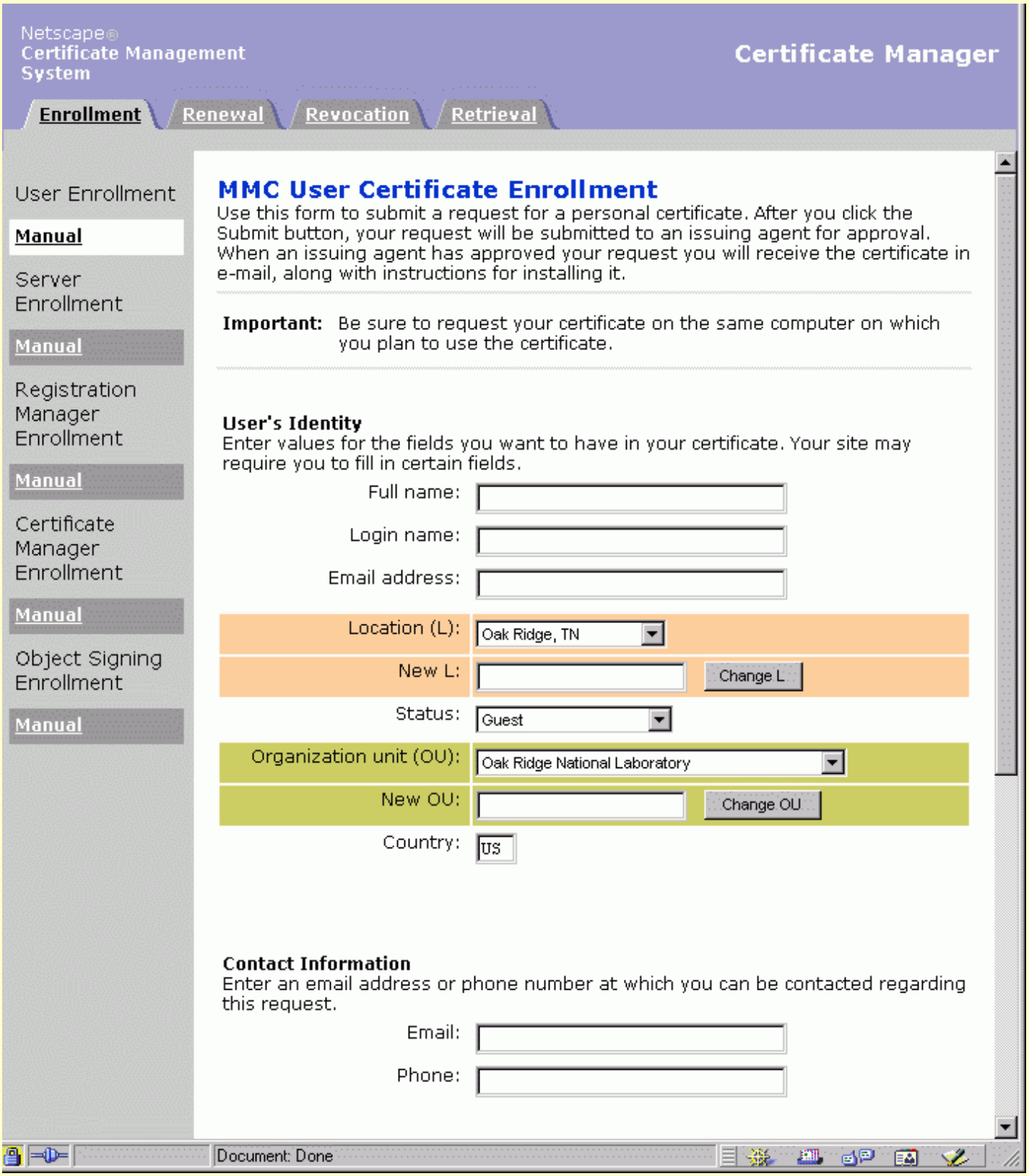
Object signing

To combat the threat of computer viruses, executable code is now being signed to prove its authenticity and integrity. Java applets and Active-

X controls are examples of the types of things that should be signed. If we create code that runs on a user's machine, it should be signed for both the user's peace of mind and for our legal protection. The Netscape *signtool* utility allows you to use MMC Client Certificates for code signing.

Certificate servers

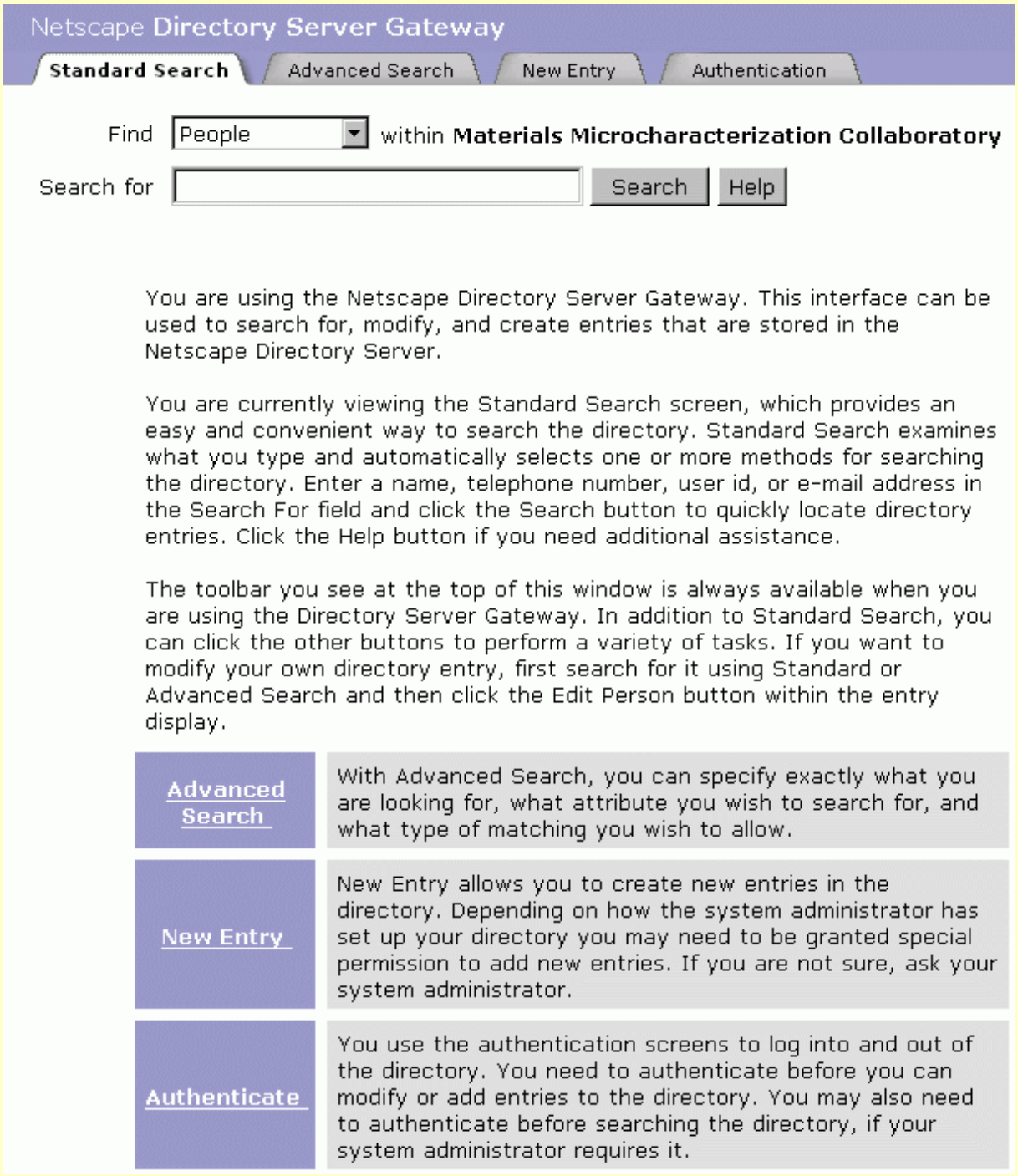
Certificate servers create, verify, renew, revoke, and reissue certificates. We are now using the Netscape Certificate Server 4.0 via a secure (https) SSL connection. You may access the MMC Certificate Server at https://mmc.cind.ornl.gov:443. It provides a public interface for requesting certificates and for accepting the MMC CA into your Netscape browser.



Document: Done

Directory services (LDAP)

To find the telephone number of someone, you use a phone directory. To find a person's public key, you use a directory server. The lightweight directory assistance protocol (LDAP) is now offered by a variety of vendors, and I have installed the Netscape LDAP server for use by the MMC. The LDAP server has many uses. From your point of view, the most useful function of the LDAP server is to allow you to find an MMC user's public key so that you can send him/her e-mail. You can query the MMC LDAP server at https://mmc.cind.ornl.gov:19149/dsgw/bin/search?context=dsgw. Of course, you need to have a user ID and password before you can modify entrieshere.



The MMC LDAP Server Gateway

The LDAP server can also be accesses by other programs and can return components of the certificate to the requesting programs. This will be used by the MMC to institute role-based access control (RBAC). In our certificates, I have used one of the fields in the certificate attributes to

contain the user's role. So instead of ST meaning *state*, for us it means *status*. There are six allowed values for status:

- *Guest* - Can observe only.
- *Student* - Can operate basic functionality of online facilities.
- *Researcher* - Can operate every allowed remote control.
- *Operator* - Facility owner with no restrictions.
- *Server* - For MMC secure Web servers
- *Administrator* - For access to secure server resources (such as the Certificate Server)

How to get your MMC certificate

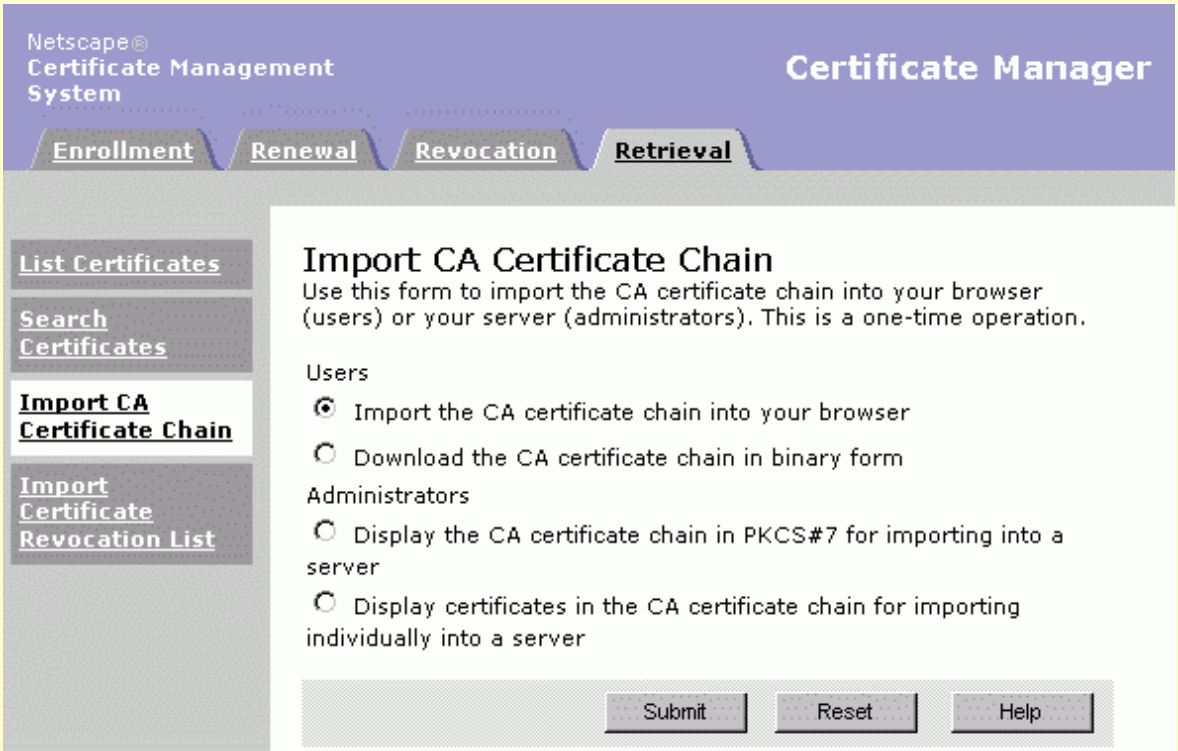
You must use Netscape Communicator, Version 4. Because the certificate format changed between versions 4.03 and 4.04, it is best to use version 4.04 or higher. I strongly suggest upgrading to Netscape 4.51 because it automatically picks the correct certificate for you to use. If you are in the US or Canada, be sure you have the 128-bit (domestic) version of Netscape installed. You can tell by accessing the *Help, About Communicator* menu and looking for the following text: *This version supports U.S. security with RSA Public Key Cryptography, MD2, MD5, RC2-CBC, RC4, DES-CBC, DES-EDE3-CBC* .

Follow these six easy steps:

1. Accept the MMC CA

In order to get Netscape to properly accept the MMC Certificate Authority, first visit the following URL: https://mmc.cind.ornl.gov:443 and access the *Retrieval* tab. I suggest that you bookmark this page. The first time you access this server, it will ask you whether you wish to accept the Server's certificate. Answer yes, and accept all options. If your Communicator refuses to connect to the https server, go into the Netscape Security Menu and under *Certificates, Web Sites*, delete any existing certificate for mmc.cind.ornl.gov.

Click on the *Import the CA certificate chain into your browser* button (as shown below) and follow the instructions. Accept it for every purpose and forever. I suggest naming this authority the *MMC CA*.



2. Apply for a certificate

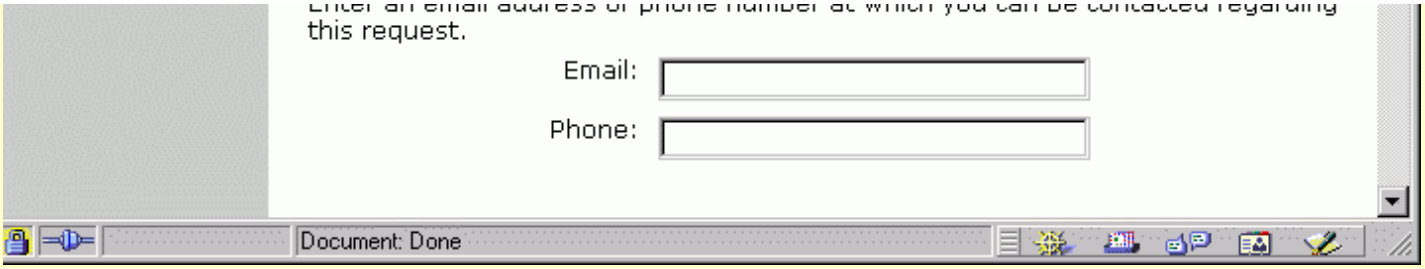
Now access the *Enrollment* tab and request a personal certificate.

Please use your full name including your middle initial. If you are not a member of one of the five MMC sites, enter the non-abbreviated names for your Organization unit (where you work) and its location in the blank entry fields and click the change buttons.
In the *additional comments* field, put the name of an MMC principal who can vouch for your identity. Be sure to send me the pop-up e-mail so that I know that an application needs to be serviced..

When you apply for a certificate, you will have to provide two passwords.

- The first one is to protect the private key that is generated in the application process (you pick it).
- The second one protects the Netscape key database. If you had certificates before, the password is the one that you used previously. If this is the first time with a certificate, you choose the password.

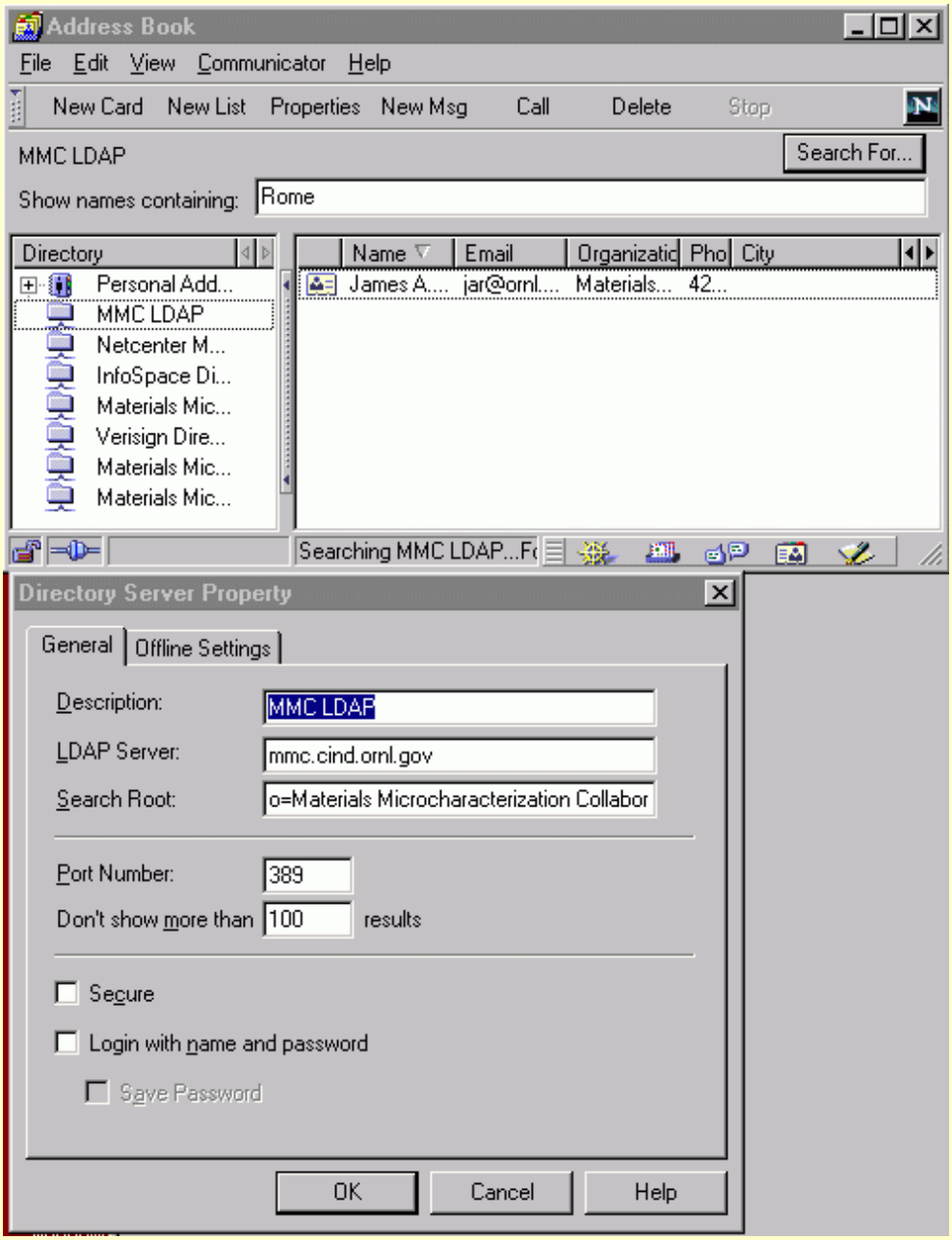
I suggest using the same password for the private key and for the key store. Don't forget the password!



Apply for an MMC certificate

3. Install the LDAP server into your Browser

Open your Netscape Address book (under the *Communicator, Address Book* menu), and under the *File, New Directory* menu, add the MMC LDAP as shown below:

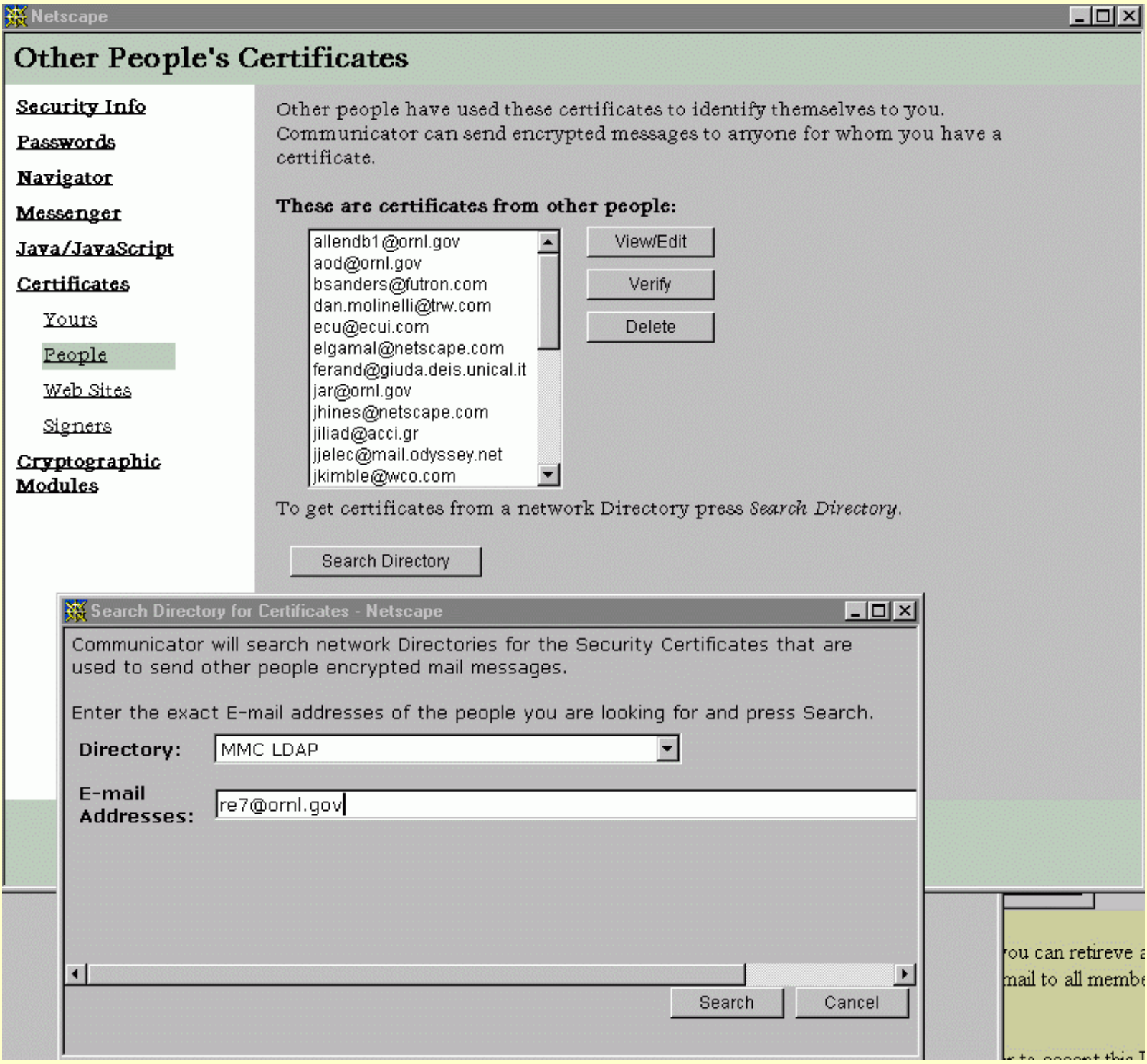


The Search Root should be: *o=Materials Microcharacterization Collaboratory*.

As shown above, once the MMC LDAP is installed, you can retireve an MMC member's information and certificate from the LDAP server.

This will enable you to send encrypted mail to all members of the MMC.

Your browser should pop up a window asking whether to accept this LDAP server. Answer yes.
You will now be able to look up MMC users in your Browser's Security menu.



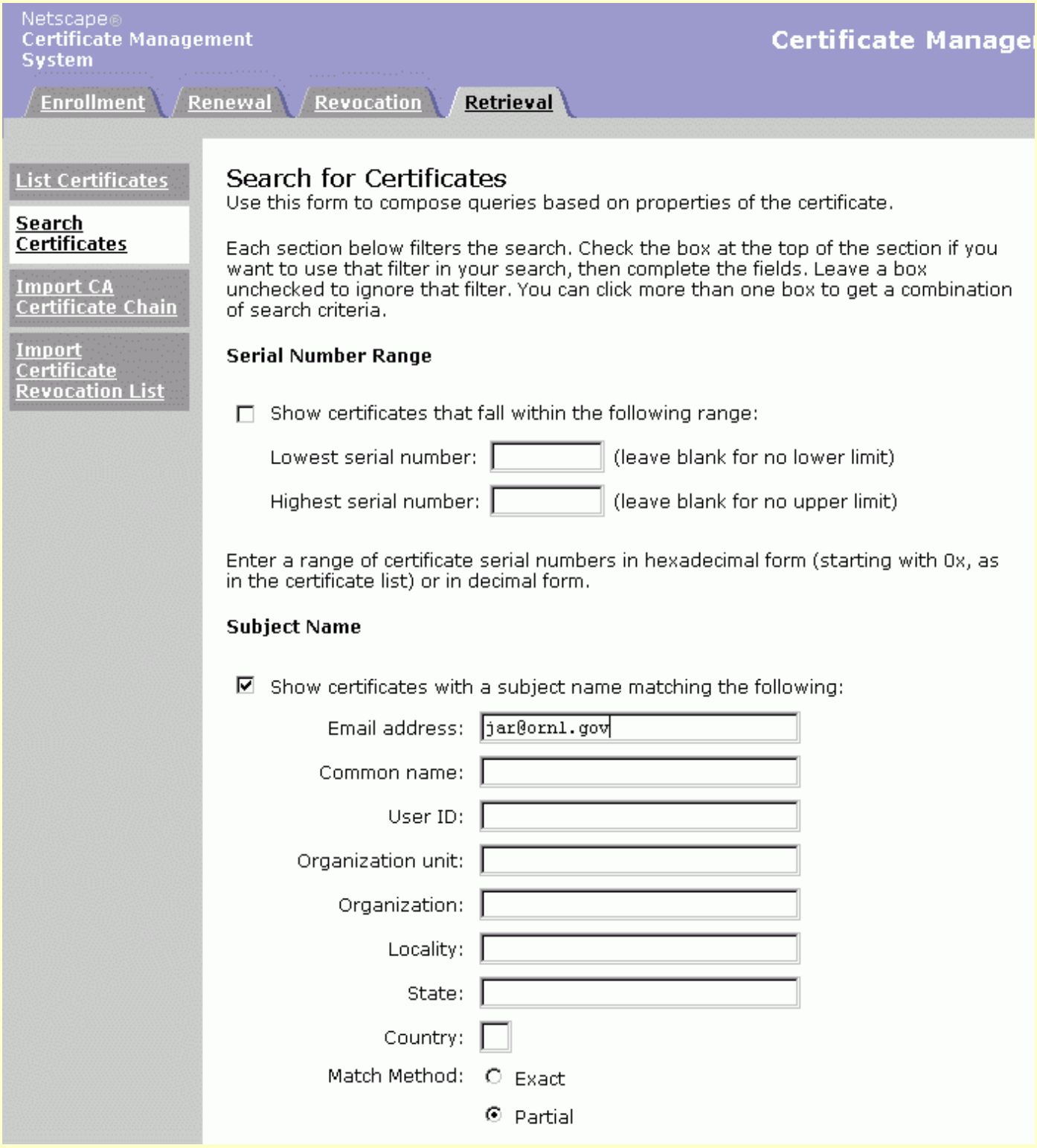
Query the LDAP server to obtain a user's public key

4. Wait for an e-mail stating that the certificate has been issued

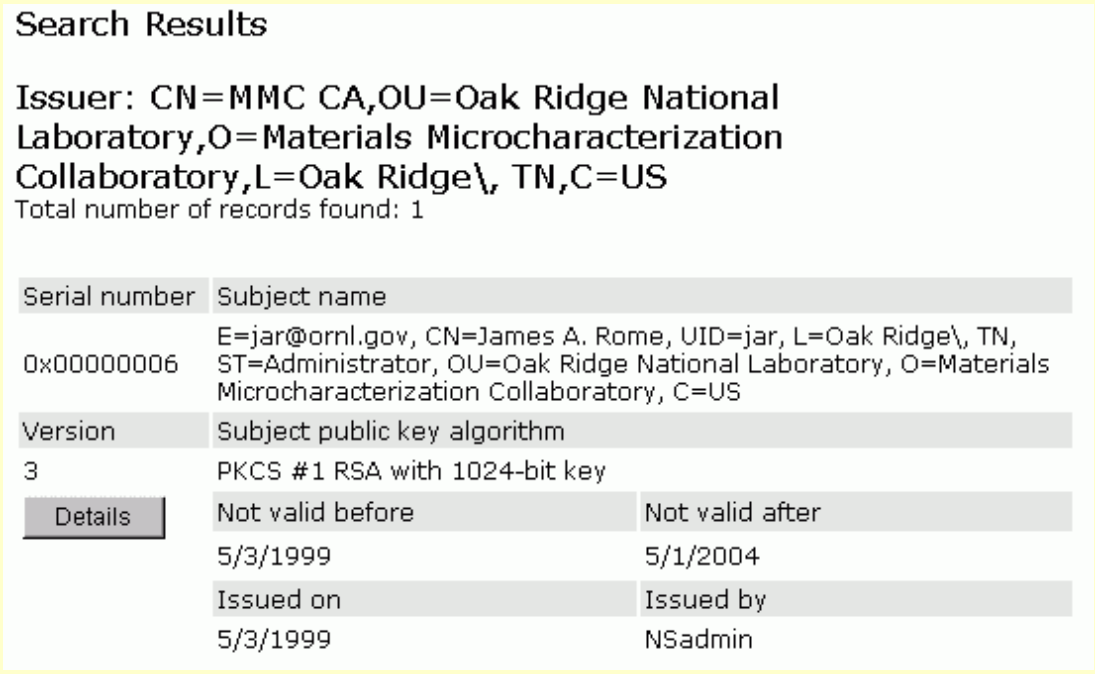
5. Retrieve your certificate

Visit the MMC CA URL (https://mmc.cind.ornl.gov:443) and under the *Retrieval* tab and search for your certificate using your e-mail address

or name.



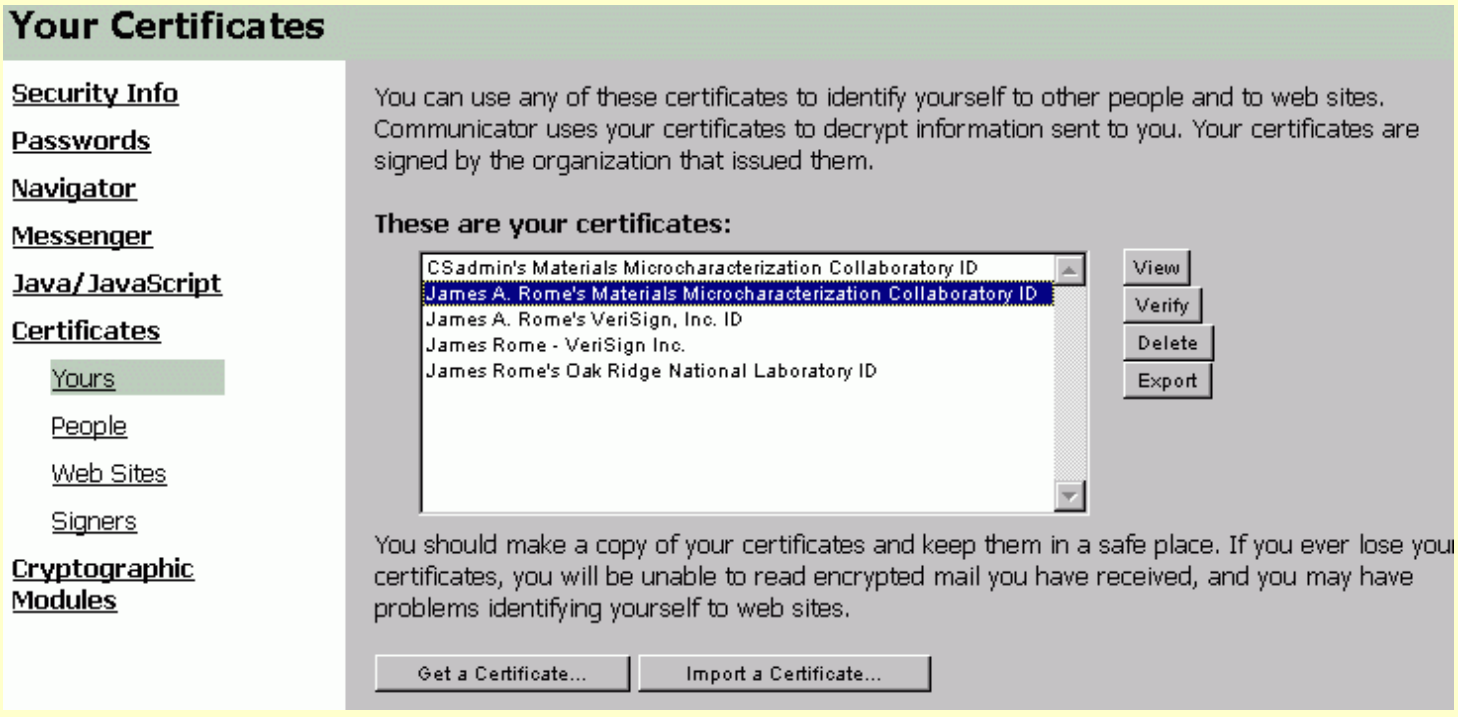
The search result will show your certificate and there wiill be a button for details:



Open the details screen and at the bottom you will find a button to import the certificate into your browser.

When you install the certificate, you will be asked whether you wish to save the certificate. **Be sure to save your certificate!!** You can export your certificate at any time using the Security menu in Communicator. The certificate is saved as a pkcs#12 crypto-wrapped file that is password protected. Use this file to transfer your certificate to all of your other Netscape Communicators.
Note: The .p12 files are upward, but not downward compatible between Communicator 4.03 and 4.04.

During the installation process, you will be asked for a password to protect your private key. In addition, if you have never installed a certificate into your Communicator you will be asked (twice!) for a password to protect the Communicator database. I suggest that to avoid confusion, you use the same password for this and for your private key.



Click on Export to save your certificate

6. Change your LDAP Password

1. Visit the LDAP server https://mmc.cind.ornl.gov:19149 and authenticate yourself with the password I mailed to you along with the certificate URL.
2. Search for yourself, and edit your record.
3. Fill in all the additional information that is relevant so that MMC members can contact you more easily.
4. Change your password on this same editing page.

Using your MMC certificate

For a tutorial on certificates in general see the talk I delivered at the ORNL Web Week in 1997:
http://mmc.cind.ornl.gov/jar/certificates/sld001.htm

Secure, certificate-based Web authentication

Visit my secure electronic notebook at https://mmc.cind.ornl.gov:444/enote/.

You can set up your web site to require and accept our certificates for access. Use the main MMC CA page to apply for a certificate for each of your servers.

Be sure to

- Accept the MMC CA into your server by visiting the MMC CA page.
- Refuse to accept certificates from other CAs.
- You can specify the CNs (common names) in the certificates that will be allowed or deneyed access to different directories. Details of how to do this depend on your server.

We should be able to use the LDAP server for more clever things. I'll update this note when I figure it all out.

Secure e-mail

Set up your Netscape Messenger (in the Security menu) so that it uses your certificate for signing and encrypting e-mail. You can also turn them off (or on) optionally in each message that you send. As stated above, I recommend that you always sign e-mail.

Netscape Messenger interface for S/MIME e-mail

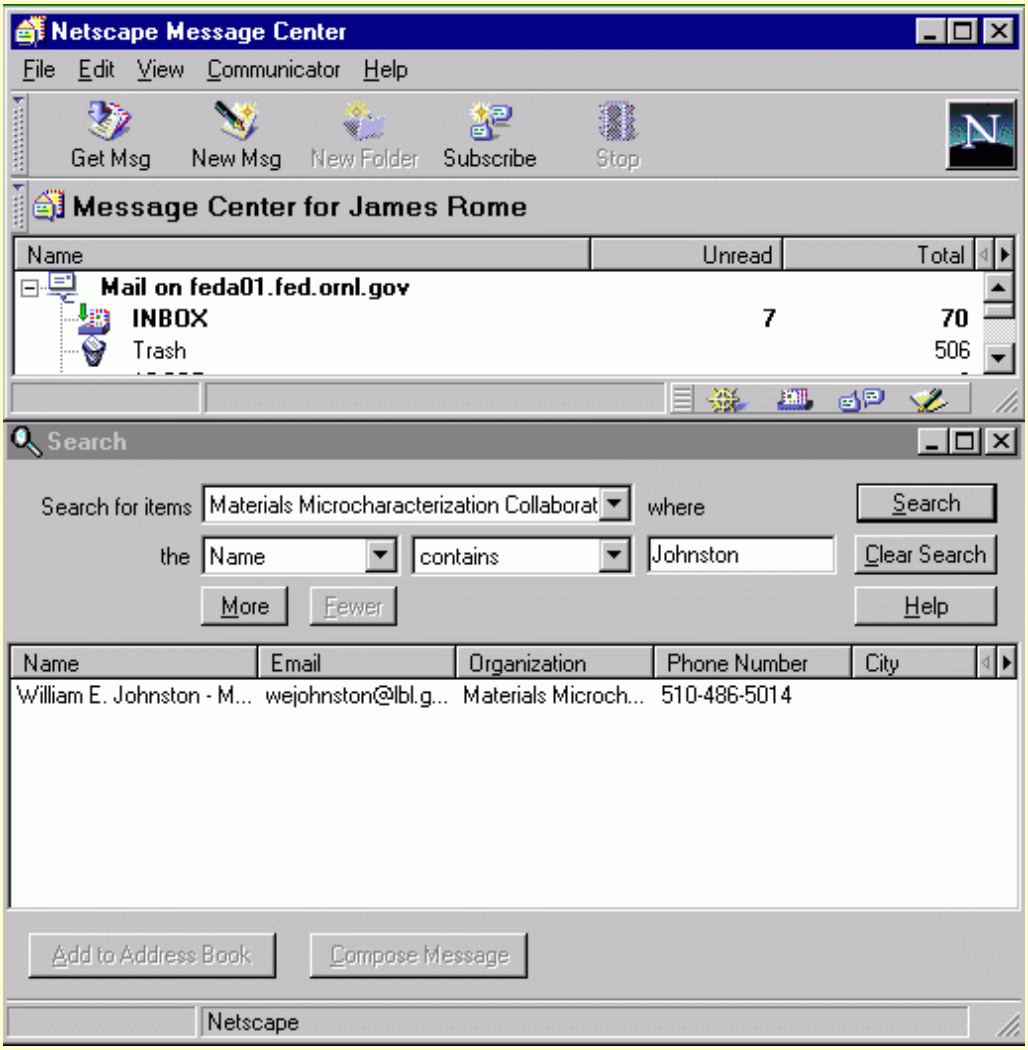
If you receive signed S/MIME mail from someone, Netscape will automatically extract their public key and save it so that you can send them encrypted mail in the future. That's another good reason for signing your mail. Or, if the user has an MMC certificate, you can use Communicator to look it up in the LDAP server as outlined above. Attachments are also encrypted.

Publish your certificate

In the above screen, you can publish your certificate in other directory servers so that people outside the MMC can find you. This may or may not work because of the way we have changed the definition of the ST (State) field.

Search the directory

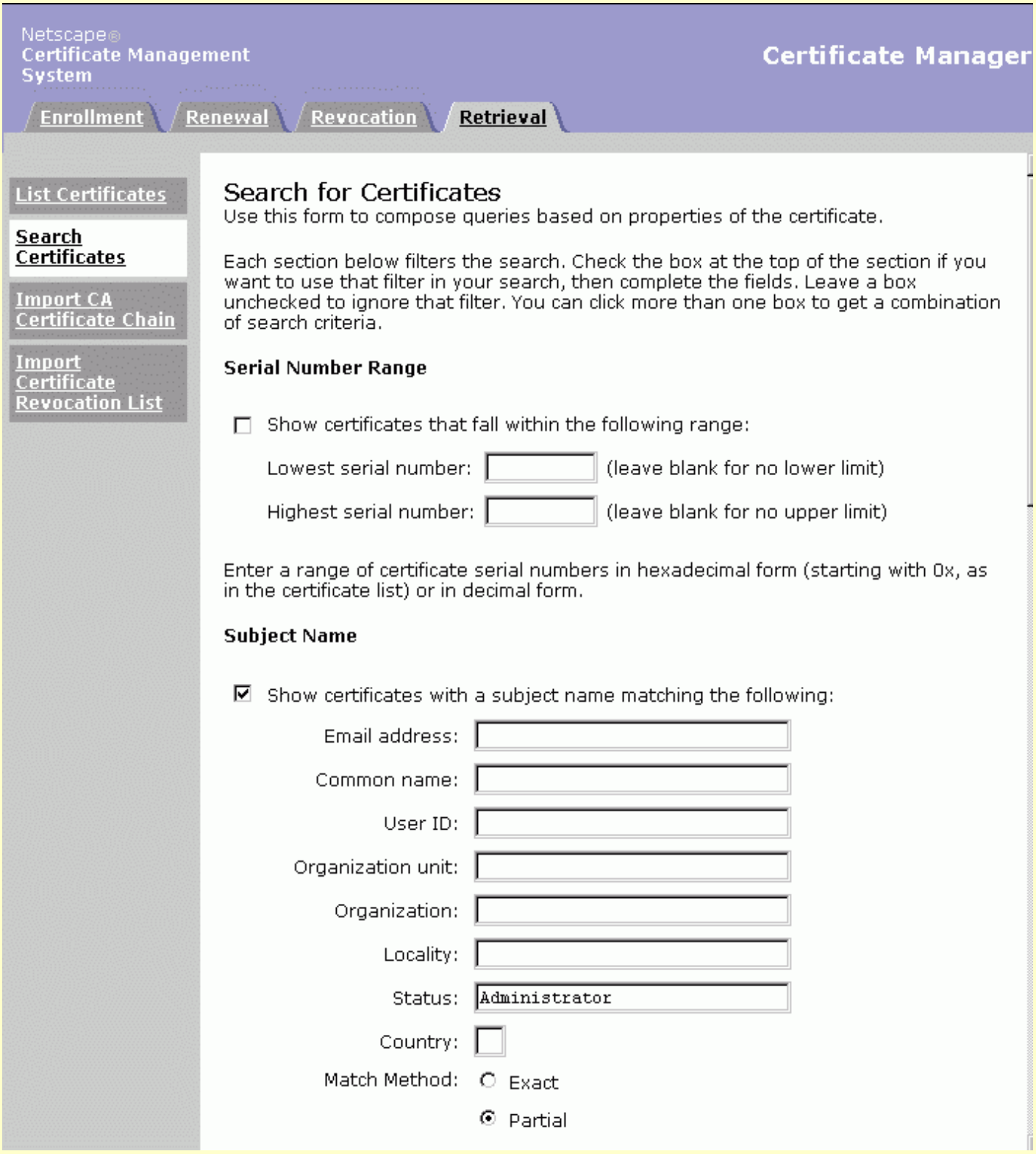
You can access and search the MMC LDAP via the Netscape Messenger. Under the *Edit* menu, select *Search Directory*.



Searching the MMC LDAP server

Search the certificate server

You can search the certificate server directly to find out *all* the information in a person's certificate. In many ways this is preferable to searching the LDAP server because information in the certificate is certified (i.e., cryptographically signed the the CA — me). For example, below I search for all certificates issued to people with the status of "Administrator":



Searching for certificates for "Administrator" using the Certificate Server

---

Internet Explorer Advice

IE users should consult InternetExplorer.html.