PKI Certificates — What are they? How do I get and use them?

20th DoE Computer Security Group Training Conference

April 27, 1998

James A. Rome

Oak Ridge National Laboratory

jar@ornl.gov

http://www.epm.ornl.gov/~jar

Certificate functions

- Strong authentication
  - An external authority vouches for your "identity."
- It contains the public key of the certificate holder that allows another entity to encrypt messages that only the certificate holder can decrypt.
- It is the foundation of privacy and security on the Internet.
  - electronic commerce
  - encrypted transmissions

My VeriSign certificate

Netscape

Your Certificates

Security Info

Passwords

Navigator

Messenger

Java/JavaScript

Certificates

Yours

People

Web Sites

Signers

Cryptographic Modules

You can use a
Communicator
signed by the c

These are yo

CSadmin's
James A.
James A.
James Ro
James Ro
test1's Ma

You should ma
your certificate
have problems

Get a Cert

View A Personal Certificate - Netscape

This Certificate belongs to:
James A. Rome
jar@ornl.gov
Digital ID Class 1 - Netscape Full Service
www.verisign.com/repository/CPS Incorp. by Ref.,LIAB.LTD(c)96
VeriSign Class 1 CA - Individual Subscriber
VeriSign, Inc.
Internet

This Certificate was issued by:
VeriSign Class 1 CA - Individual
Subscriber
VeriSign, Inc.
Internet

Serial Number: 60:BE:2F:8D:42:AB:BF:DE:88:D0:2E:A7:B6:B4:DA:F6
This Certificate is valid from Mon May 05, 1997 to Wed May 06, 1998
Certificate Fingerprint:
94:59:C0:A9:B3:43:4B:0F:3F:C4:76:E5:92:B7:F0:90
Comment:

CAUTION: The Common Name in this Class 1 Digital
ID is not authenticated by VeriSign. It may be the
holder's real name or an alias. VeriSign does auth-
enticate the e-mail address of the holder.

OK

Oak Ridge National Laboratory

Public and private keys

Keys are the two parts of a mathematical operation that is easy to do if you know both parts, but computationally intensive to crack if you only know one.

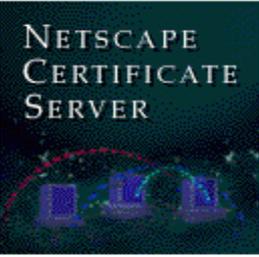- ⌘ Prime factors of large (1024 bit) polynomials
- ⌘ Discrete logarithms

The details are unimportant, but the two numbers become your

- ⌘ public key - available to the world
- ⌘ private key - ***known only to you and kept securely***

How do you get keys and certificates?

⌘Keys are generated on your PC because the private key should never leave your possession.

- ◆ Can be done by a Web browser or an application program such as PGP, SSH,….

⌘To get a certificate for your browser, visit the Web site of a Certificate Authority (CA) and apply for a certificate. You might have to

- ◆ submit proof of identity
- ◆ pay a fee
- ◆ appear in person

Oak Ridge
National Laboratory

Getting a certificate

Each CA package uses its own user interface

Applying for a certificate

Getting the certificate

It is a good idea to save a copy of the certificate when Netscape gives you that option.
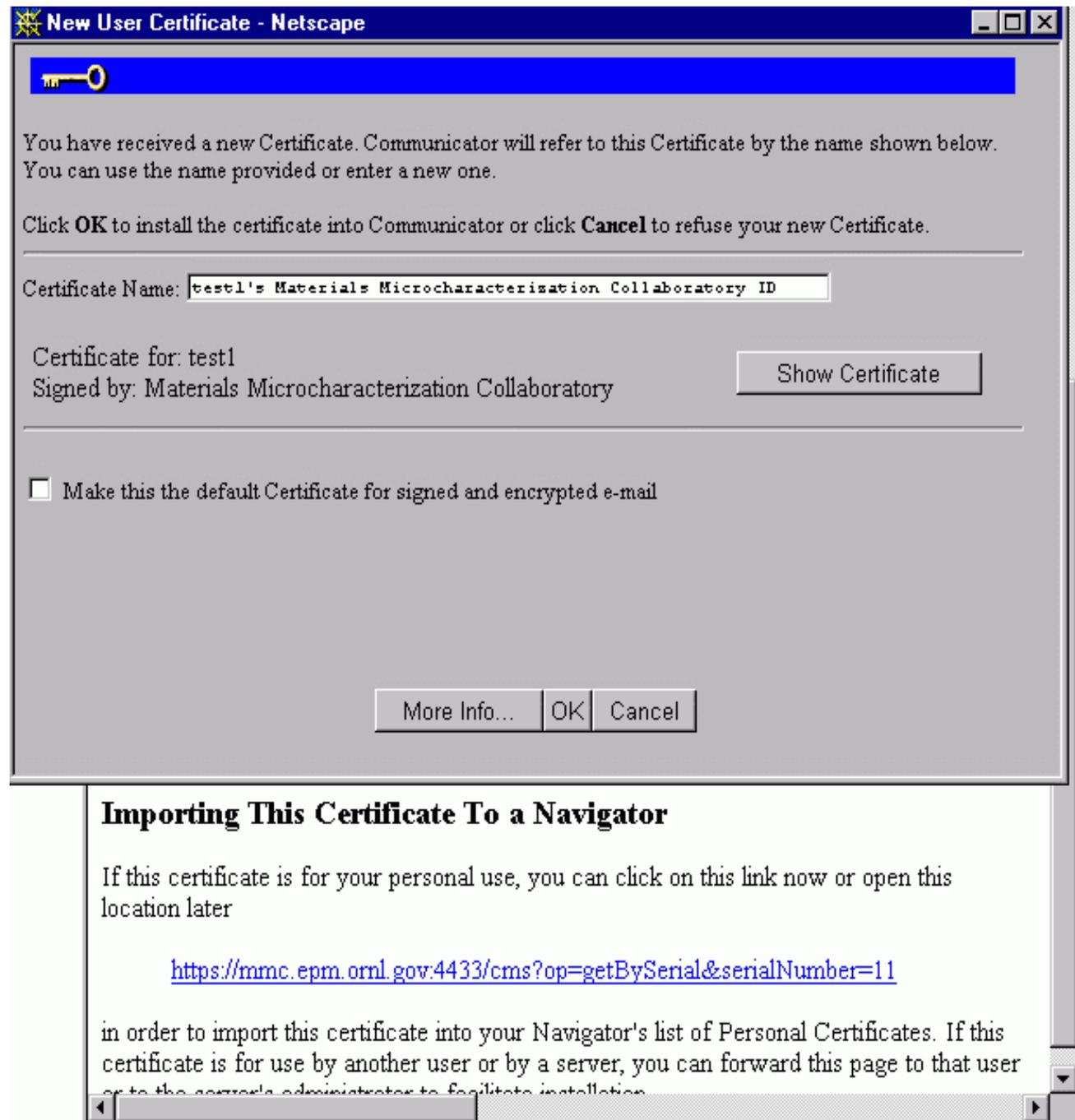
New User Certificate - Netscape

You have received a new Certificate. Communicator will refer to this Certificate by the name shown below. You can use the name provided or enter a new one.

Click **OK** to install the certificate into Communicator or click **Cancel** to refuse your new Certificate.

Certificate Name: test1's Materials Microcharacterization Collaboratory ID

Certificate for: test1
Signed by: Materials Microcharacterization Collaboratory

Show Certificate

☐ Make this the default Certificate for signed and encrypted e-mail

More Info... | OK | Cancel

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://mmc.epm.ornl.gov:4433/cms?op=getBySerial&serialNumber=11

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

What's in a certificate?

⌘ The Subject Name (Distinguished Name, or DN) contains the information that distinguishes the user's "identity."

⌘ It also contains the holder's public key.

⌘ The certificate is signed by the CA with its private key.

⌘ The DN info is available to the Web server

Subject Name: E=test1@ornl.gov, CN=test1, UID=test1, OU=Oak Ridge National Laboratory, O=Materials Microcharacterization Collaboratory, L="Oak Ridge, TN", ST=Guest, C=US

Details

Revoke

Serial Number: 0x00000011   **Version:** 3

Not Valid Before: 3/14/98   **Not Valid After:** 9/10/98

Issued on: 3/14/98   **Issued by :** CSadmin

Subject Public Key Algorithm: PKCS #1 RSA Encryption with 1024-bit key

Digital signatures

With your certificate and keys, you can create a digital signature. This allows you to:

- Sign documents to assure that they were not forged

- Make a secure hash of a document to ensure that it was not changed

- Encrypt a document to ensure privacy

Oak Ridge National Laboratory

Commerce on the internet

Present E-commerce uses site certificates and SSL (secure sockets layer) to provide encryption.

You visit a Web site and wish to make a purchase. What needs to be known?

- ⌘ Is the site really LL Bean, or an imposter?

- ⌘ Will the transaction be encrypted so that your credit card is secure?

- ⌘ You identity is implicit because if the credit card is accepted, the merchant is protected.

Unsecure site (http://…)

Secure site (https://....)

Secure site's certificate

This site processes secure orders for Readmedotdoc.com

Online Certificate Status Protocol

Netscape ☒

OCSP Settings

Personal Security Manager can use the Online Certificate Status Protocol(OCSP) to verify certificates.
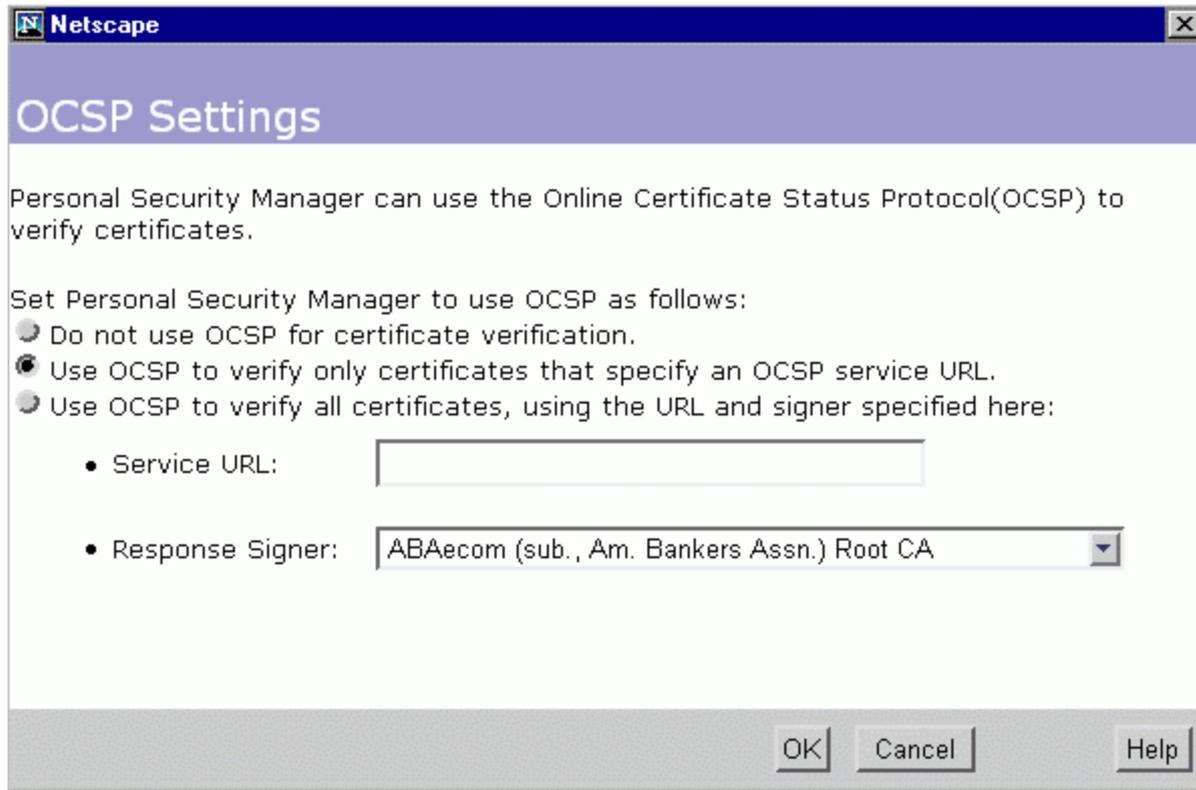
Set Personal Security Manager to use OCSP as follows:

- ○ Do not use OCSP for certificate verification.
- ● Use OCSP to verify only certificates that specify an OCSP service URL.
- ○ Use OCSP to verify all certificates, using the URL and signer specified here:

  - Service URL: [   ]

  - Response Signer: [ABAecom (sub., Am. Bankers Assn.) Root CA ▼]

[OK] [Cancel] [Help]

OCSP makes it possible for the Netscape 6 Personal Security Manager to perform an online check of a certificate's validity each time the certificate is viewed or used.

E-Commerce — Details

- Look for the key or lock in Netscape.
- Examine the site's certificate.
- Your browser uses the site's public key to encrypt a symmetric session key and sends it to the server.
- The server decrypts the symmetric session key (with its private key) and uses it to create the SSL encrypted session.
- When you transmit your data, it is secure (if you trust the host company).

What does a CA guarantee?

There are different classes of certificates.

- ⌘ Commercial certificates cost money (~$300 up) and require lots of proof —Dunn & Bradstreet report, Letter from company president,…
  - ◆ VeriSign provides insurance for fraud losses
- ⌘ Personal certificates are free or cheap ($10/year) and bind an identity to an E-mail address. VeriSign gives $1000 insurance.
- ⌘ Site-issued certificates may be more appropriate for labs. (cost is $1 to $157).

What can I do with *my* certificate?

Netscape Communicator supports S/MIME E-mail
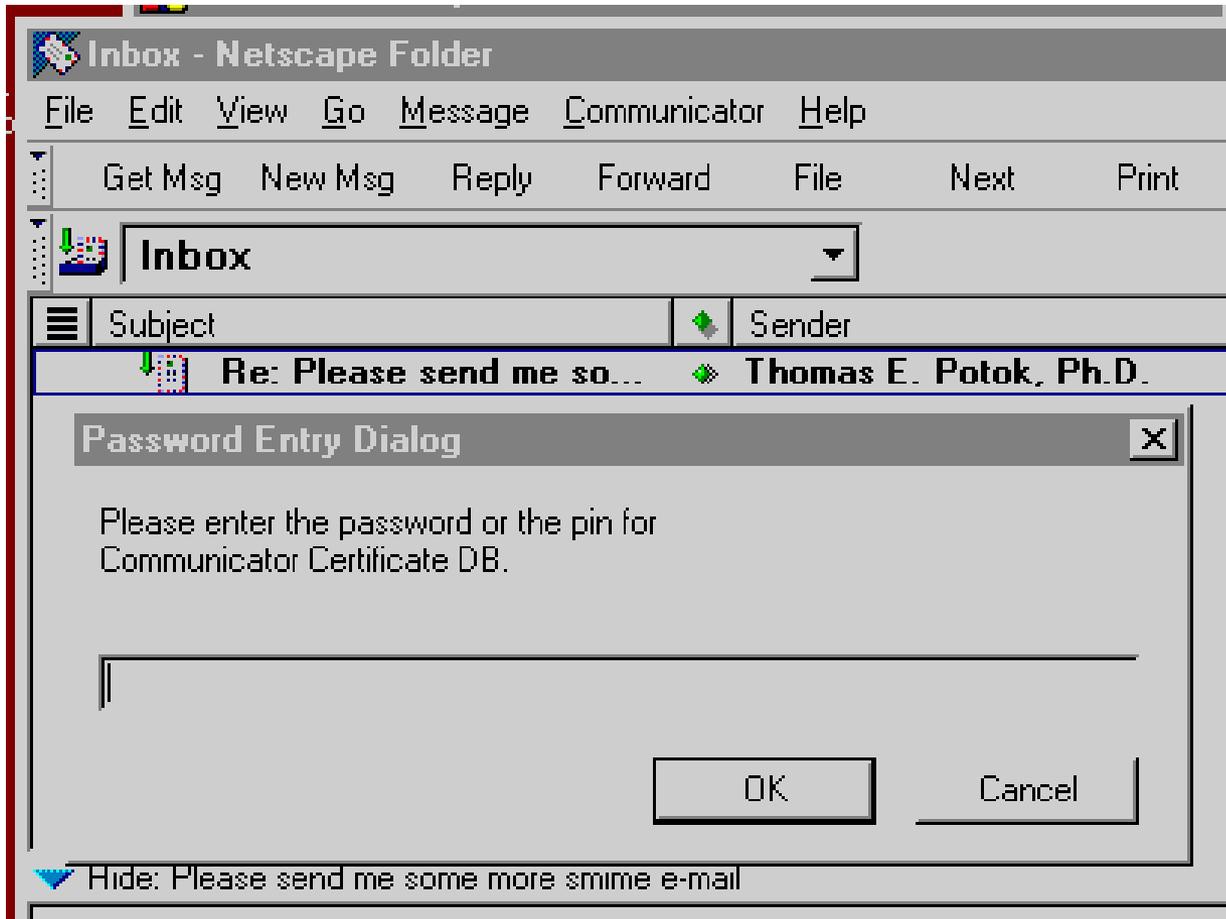
Default S/MIME settings

Messenger

Security Info

Passwords

Navigator

Messenger

Java/JavaScript

Certificates

   Yours

   People

   Web Sites

   Signers

Cryptographic Modules

These settings allow you to control Messenger security settings.

Messenger Security warnings can let you know before you do something that might be unsafe.

Sending Signed/Encrypted Mail:

☑ Encrypt mail messages, when it is possible

☑ Sign mail messages, when it is possible

☐ Sign discussion (news) messages, when it is possible

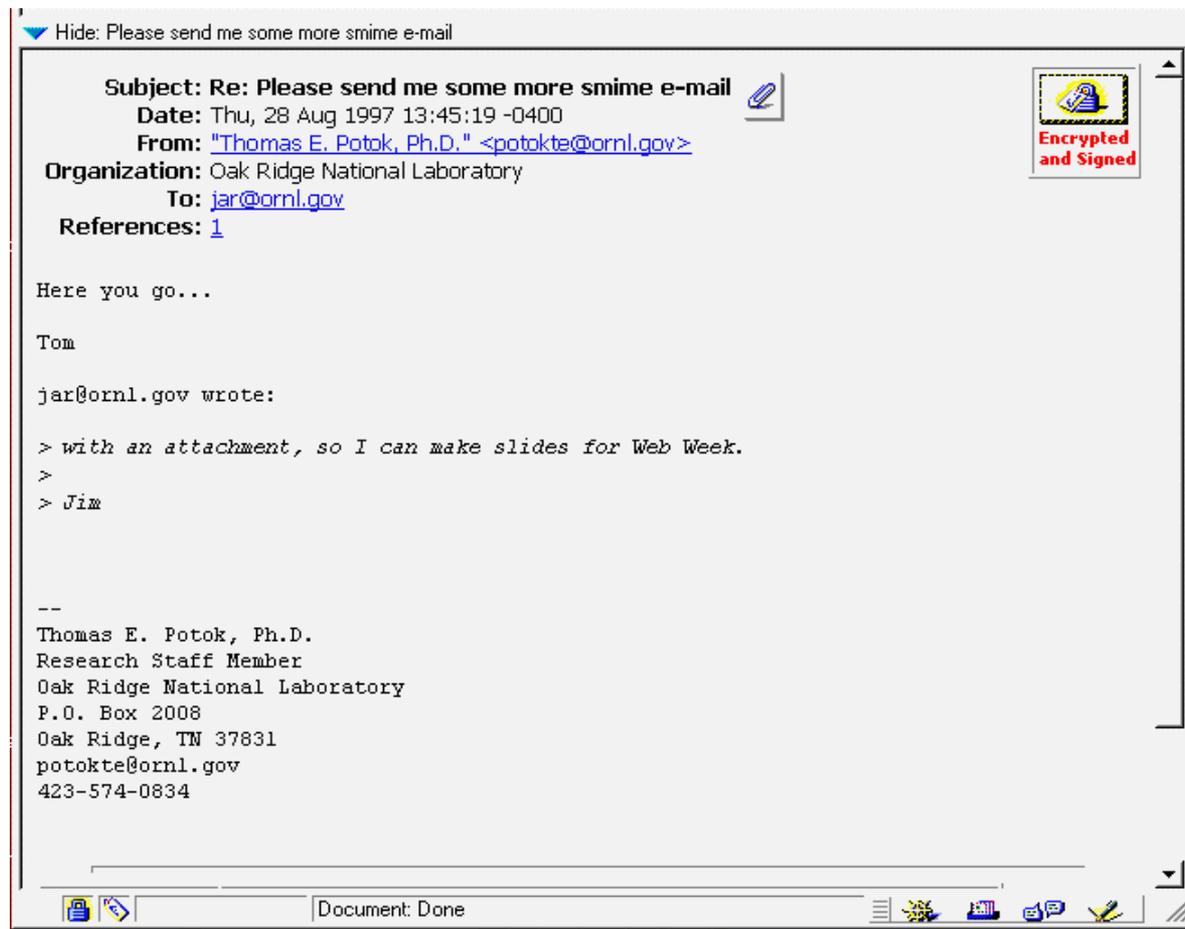**Certificate for your Signed and Encrypted Messages:**

James A. Rome's Materials Microcharacterization Collaboratory ID ▾

This certificate is included with every email message you **sign**. When other people receive it, it makes it possible for them to send you encrypted mail.Other people could also obtain your certificate from a Directory:

Advanced S/MIME Configuration:

   Cipher Preferences:

S/MIME E-mail

S/MIME E-mail

Netscape _ □ ×

Security Info

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

Encrypted Message

This message **was encrypted** when it was sent.

This means that it was hard for other people to eavesdrop on your message while it was being sent.

The algorithm used was 40-bit RC2-CBC.

Signed Message

This message **was digitally signed** by **Tom Potok** on Thu Aug 28 13:45:20 1997.

To check the Certificate, press the ``View'' button.

This Certificate has automatically been added to your list of People's Certificates to make it possible for you to send secure mail to this person.

View

OK   Cancel   Help

Oak Ridge National Laboratory

Certificates also verify downloads

How do I find a person's certificate?

If you want to send encrypted information to someone, you need to have a copy of their public key which is contained in their certificate.

Certificate Directories act like telephone books, but store people's certificates

- ⌘X.500 directory
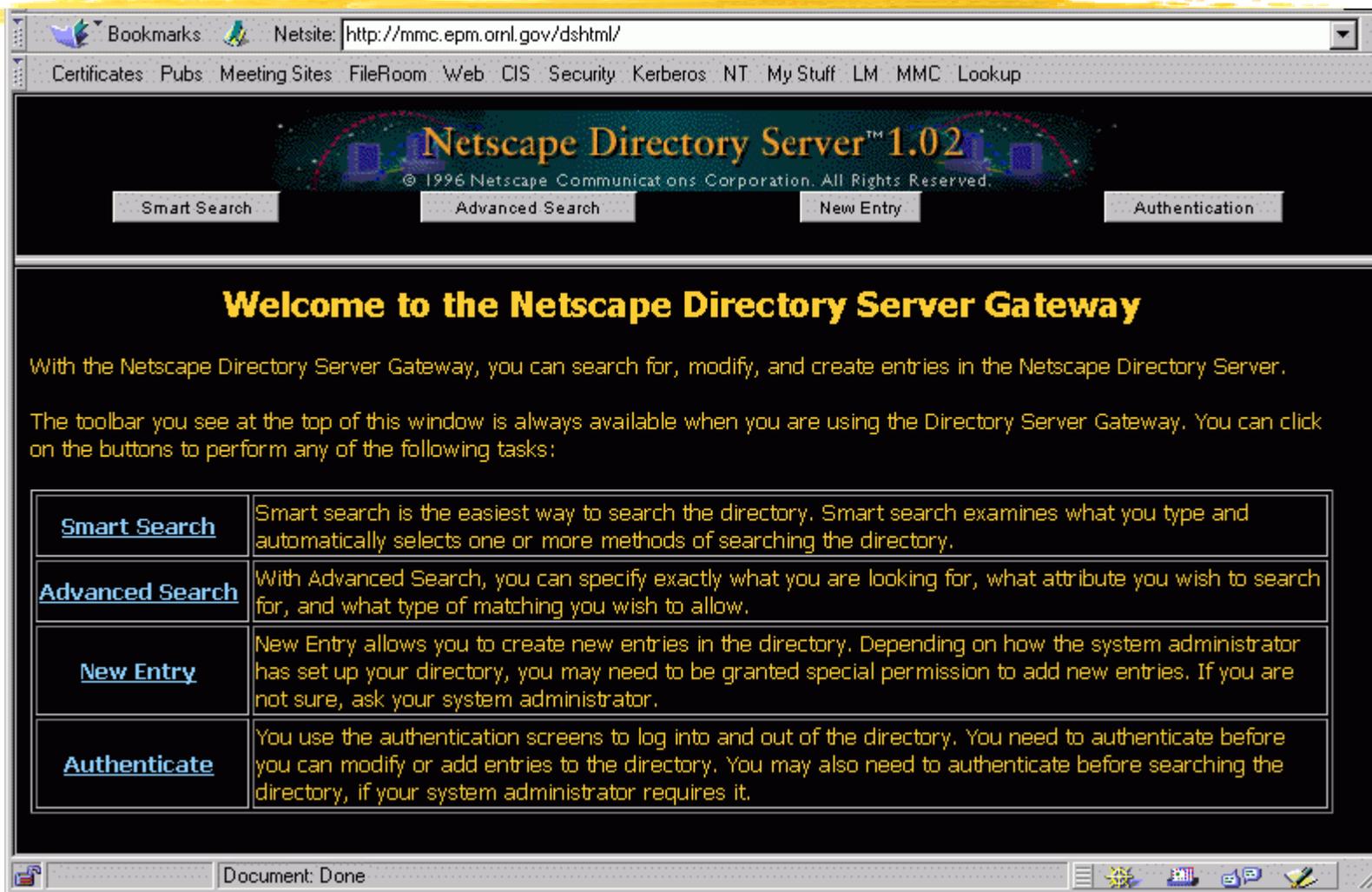
- ⌘Light-weight directory assistance protocol (LDAP)

Which John Smith do you really mean?

LDAP vs Certificate Server

Certificates can be obtained by querying either server, so why LDAP?

- ⌘LDAP contains more information so that (maybe) you can pin down John Smith.
  - ◆ Phone number, FAX number, home address, title,…
- ⌘LDAP can be modified by the user to keep his information up to date.
- ⌘LDAP is often used by an organization to maintain all employee data.

LDAP interface

Accessing an LDAP in Netscape

You can import a new LDAP server into Netscape:

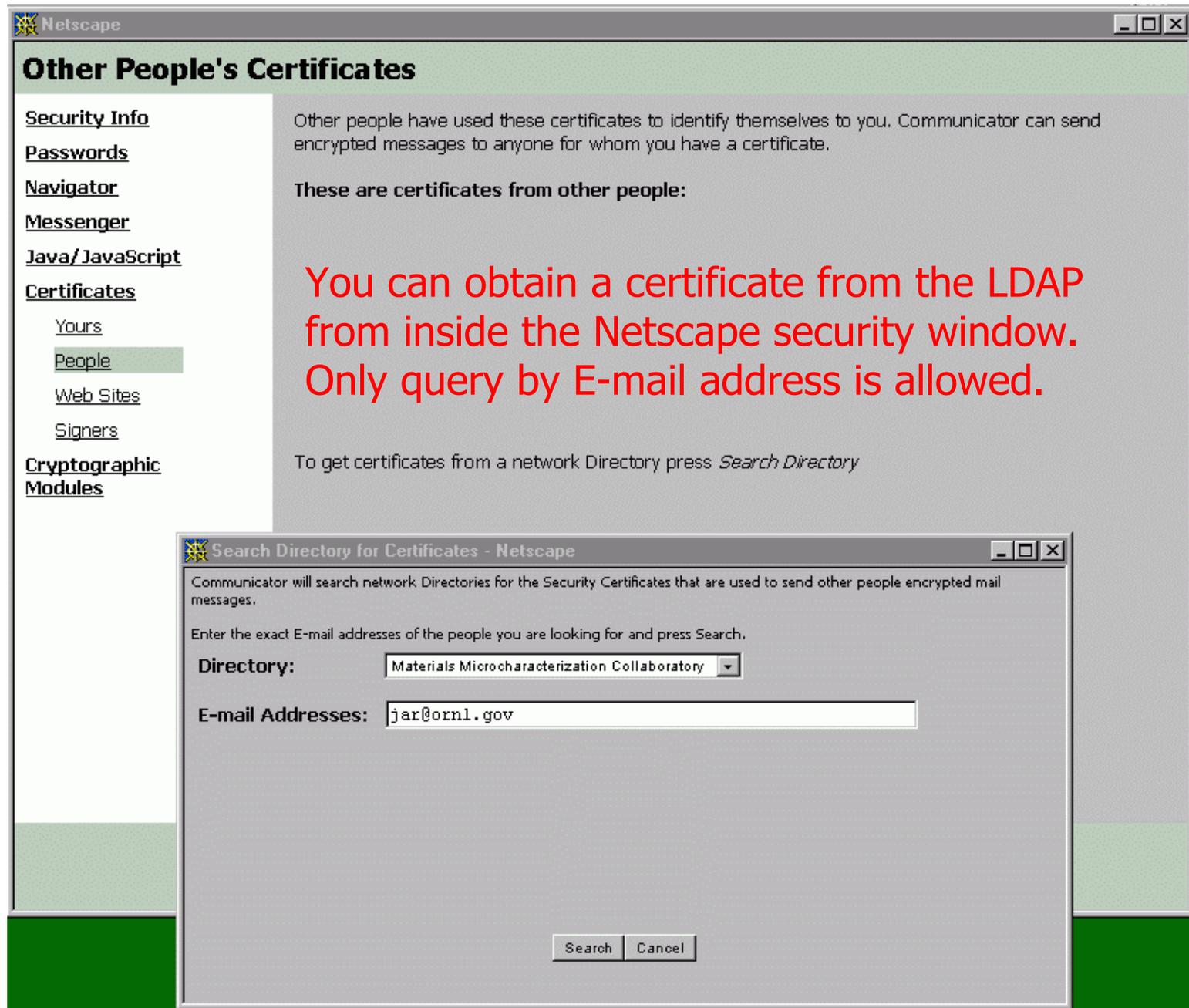⌘ For my LDAP, access the following URL:

ldap://mmc.epm.ornl.gov:389/o%3DMaterials%20Microcharacterization

%20Collaboratory%2C%20c%3DUS

⌘ The complicated argument specifies the LDAP root hierarchy.

◆ All MMC DNs have C=US, O=Materials Microcharacterization Collaboratory

⌘ Your browser should pop up a window asking whether to accept this LDAP server. Answer yes.

Other People's Certificates

Other people have used these certificates to identify themselves to you. Communicator can send encrypted messages to anyone for whom you have a certificate.

These are certificates from other people:

You can obtain a certificate from the LDAP from inside the Netscape security window. Only query by E-mail address is allowed.

To get certificates from a network Directory press *Search Directory*

Search Directory for Certificates - Netscape

Communicator will search network Directories for the Security Certificates that are used to send other people encrypted mail messages.

Enter the exact E-mail addresses of the people you are looking for and press Search.

Directory: Materials Microcharacterization Collaboratory ▾

E-mail Addresses: jar@ornl.gov

Search   Cancel

You can also formulate more complicated queries using Netscape's Messenger.

In the *Edit* Menu, select *Search Directory*.
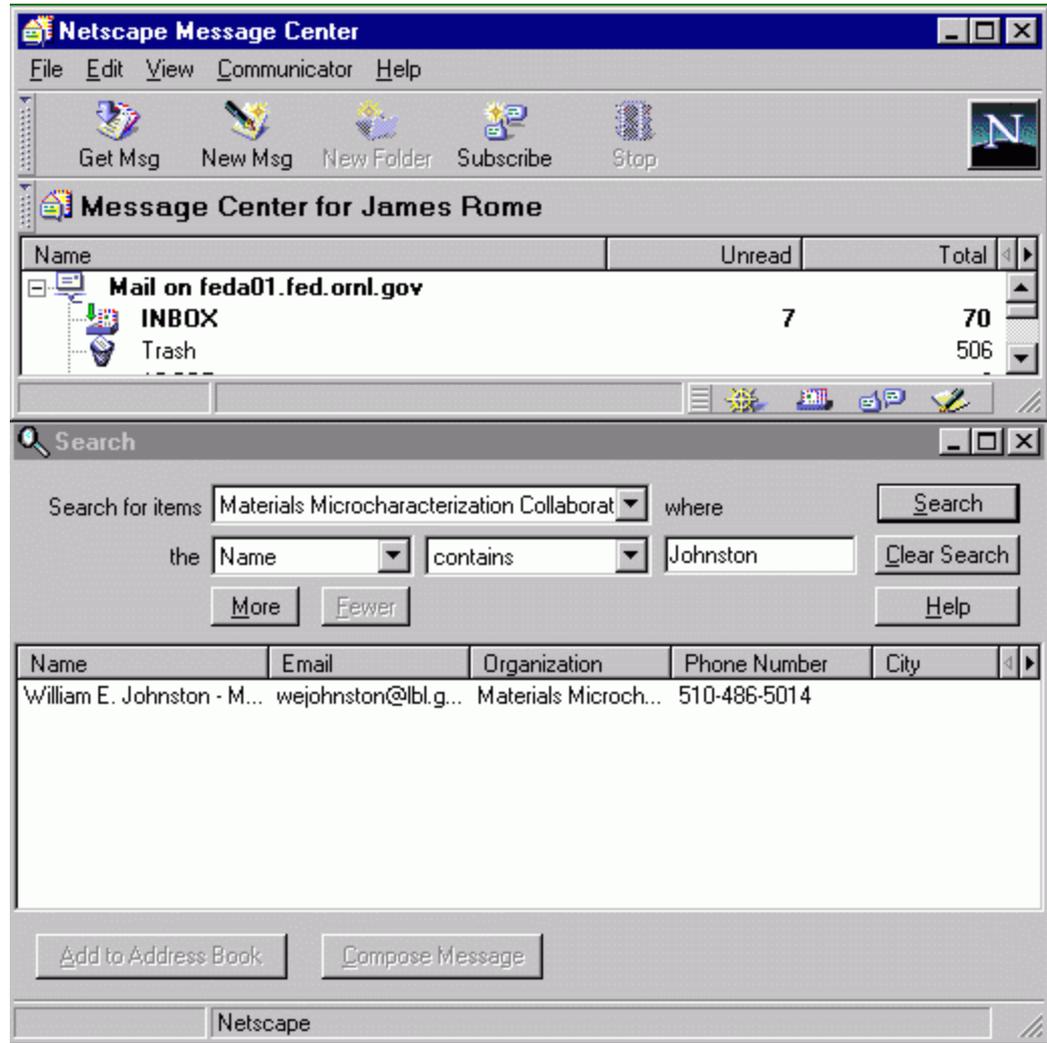
New PKI applications are coming

⌘ Eudora now supports Entrust certificates.

⌘ SET (secure electronic transaction) technology from MasterCard/Visa will enhance e-commerce

- ◆ The merchant never sees your credit information
- ◆ Both you and the merchant deal with MC/Visa as an intermediary

Other kinds of certificates

SPKI (simple public key infrastructure) certificates bind a public key to an authority.

So, to run an online facility, you need certificates that attest that:

- ⌘You have taken and passed training
- ⌘You have paid for a session
- ⌘You have a reservation for the time slot
- ⌘Your data is proprietary
- ⌘See my talk on Wednesday for details…