

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

The image shows a Netscape browser window titled "Your Certificates" with a sidebar menu containing links for Security Info, Passwords, Navigator, Messenger, Java/JavaScript, Certificates, Yours, People, Web Sites, Signers, and Cryptographic Modules. The "Yours" link is selected. A "View A Personal Certificate - Netscape" dialog box is open, displaying the following information:

This Certificate belongs to:
James A. Rome
jar@ornl.gov
Digital ID Class 1 - Netscape Full Service
www.verisign.com/repository/CPS Incorpor. 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 authenticate the e-mail address of the holder.

Buttons for "OK" and "Get a Certificate" are visible.

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

Getting a certificate




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 Certificate Revocation List](#)

Notify [Jim Rome](#) of your request



Options



Select Certificate Type


- [Browser Certificate - Generated Secret Example Type 1](#)
 - This certificate contains only your name. You can use it to identify yourself to Web sites.
- [Browser Certificate - Generated Secret Example Type 2](#)
 - This certificate contains your name, location, e-mail address, and telephone number. It can be used both to identify yourself to Web sites and to authenticate yourself when sending e-mail messages.

Each CA package uses its own user interface

Applying for a certificate

Bookmarks Netsite: <https://mmc.epm.ornl.gov:4433/>

Certificates Pubs Meeting Sites FileRoom Web CIS Security Kerberos NT My Stuff LM MMC Lookup



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 Certificate Revocation List](#)

Request a Personal Certificate

This form will help you put together the information that you need to submit a request for a [personal certificate](#).

IMPORTANT
When making this request you must use the Navigator in which you wish to use the certificate.

User's Name

Enter values for those fields that you wish to have in your certificate.
Do not abbreviate! e.g., use Oak Ridge National Laboratory *not* ORNL or Oak Ridge National Lab.

NOTE
The Status categories are: Guest, Student, Researcher, Operator

Your Full Name:

Login Name:

Your E-mail Address:

Laboratory:

City:

Status:

Country:

Check here if this certificate will be used for electronic mail.

Contact Information

Enter an e-mail address or phone number at which you can be contacted regarding this request.

E-mail:

Phone:


Additional Comments To Issuing Agent

Please write any [additional comments](#) directed to the person who will process your certificate request.


Document: Done

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:

Certificate for: test1
Signed by: Materials Microcharacterization Collaboratory

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

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 or to the correct administrator to facilitate installation.

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 | Serial Number: 0x00000011 | Version: 3 |
| Revoke | 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

Commerce on the internet

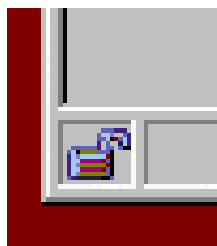
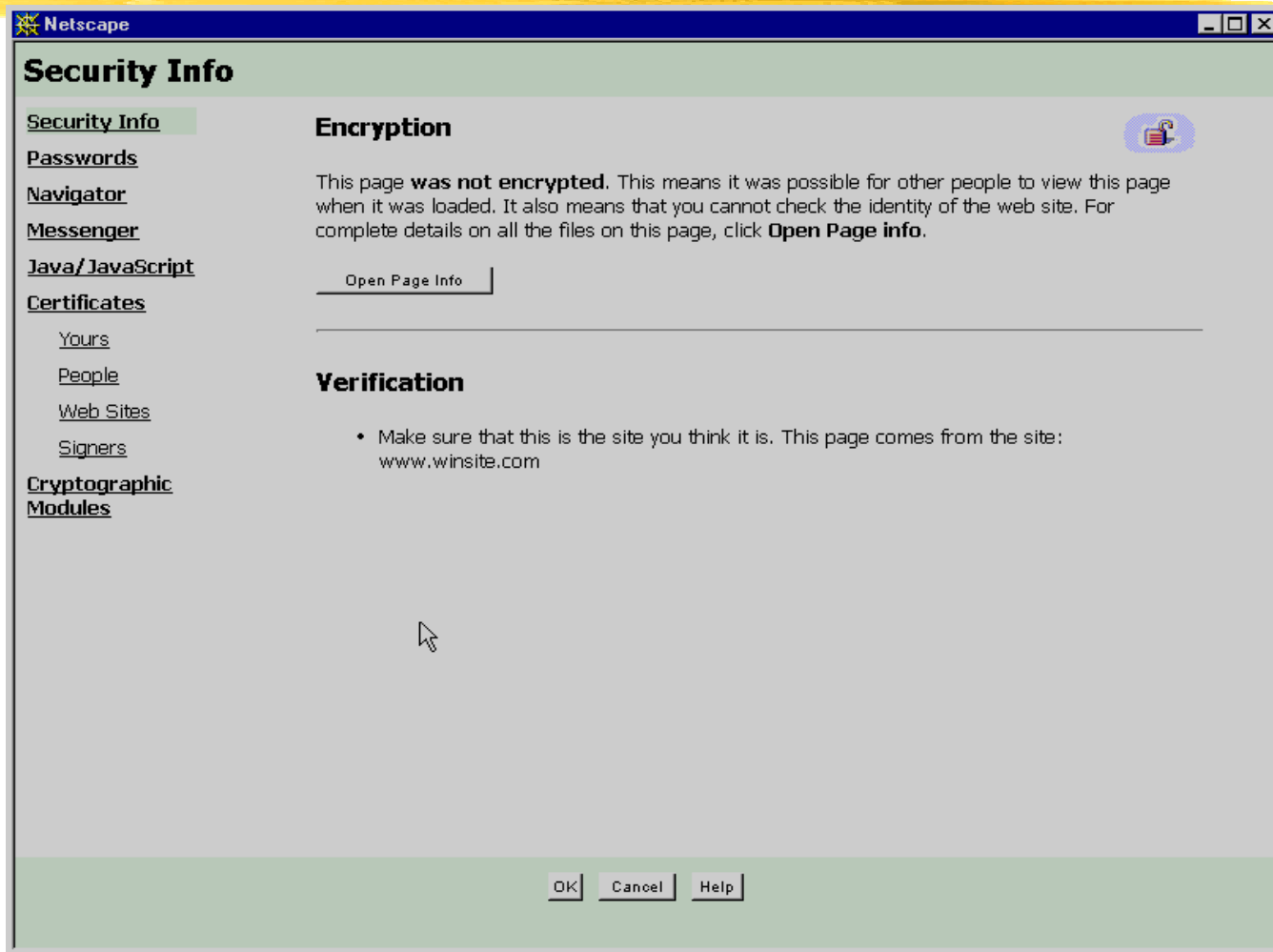


Present E-commerce uses site certificates and SSL (secure sockets layer) to provide encryption.

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

Unsecure site (http://...)



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



Secure site's certificate



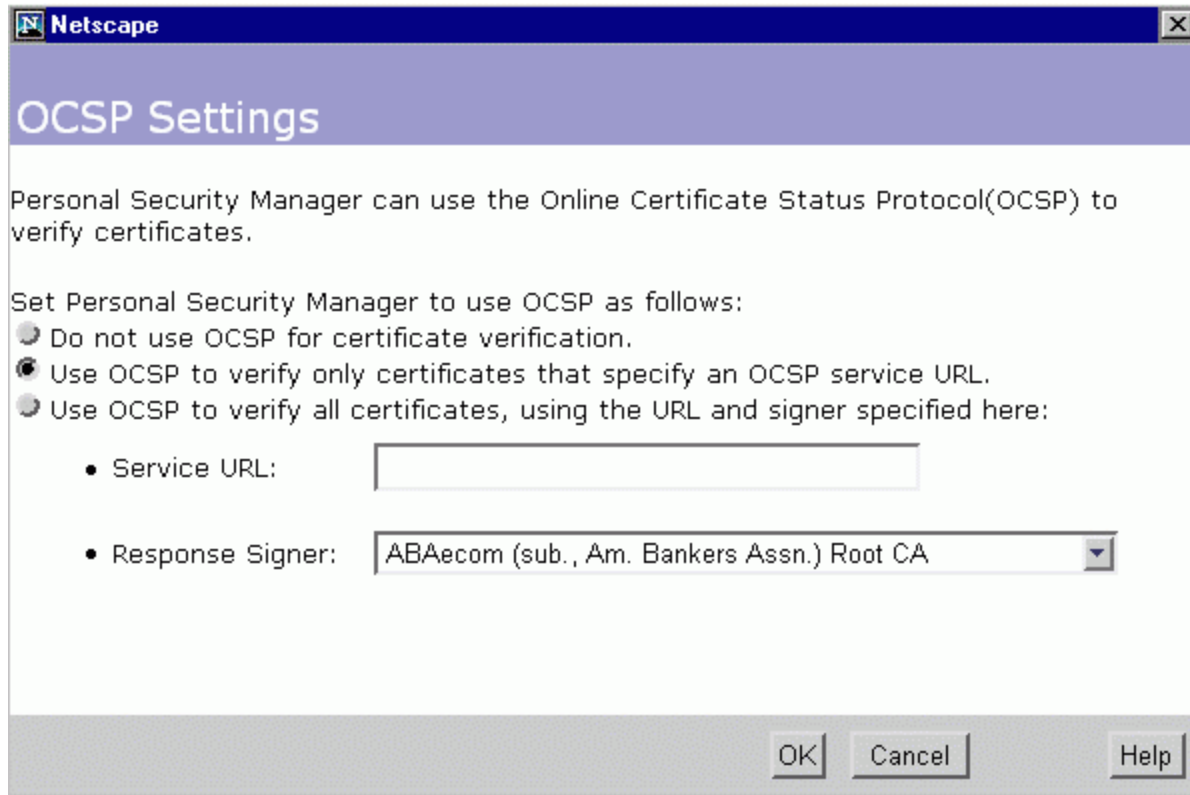
 View A Certificate - Netscape

| | |
|---|--|
| This Certificate belongs to: starshine.digiweb.com Digiweb Inc. Maryland , US | This Certificate was issued by: Secure Server Certification Authority RSA Data Security, Inc. US |
|---|--|

Serial Number: 02:F3:00:06:BD
This Certificate is valid from Sun Dec 29, 1996 to Tue Dec 30, 1997
Certificate Fingerprint:
E7:E0:F8:83:7E:63:CC:C9:8E:24:16:8F:D1:BF:80:C4

This site processes secure orders for Readmedotdoc.com

Online Certificate Status Protocol



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).

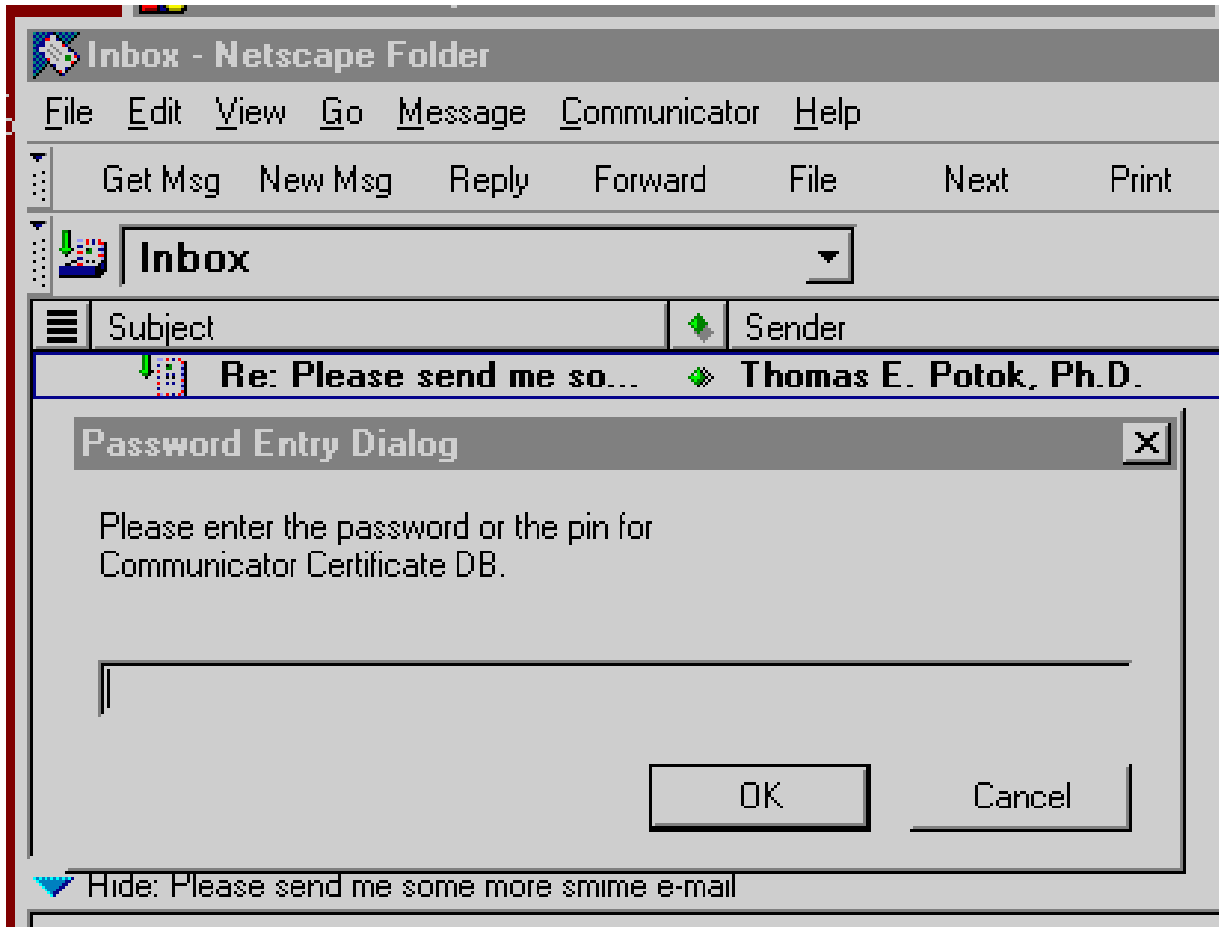
What does a CA guarantee?

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:

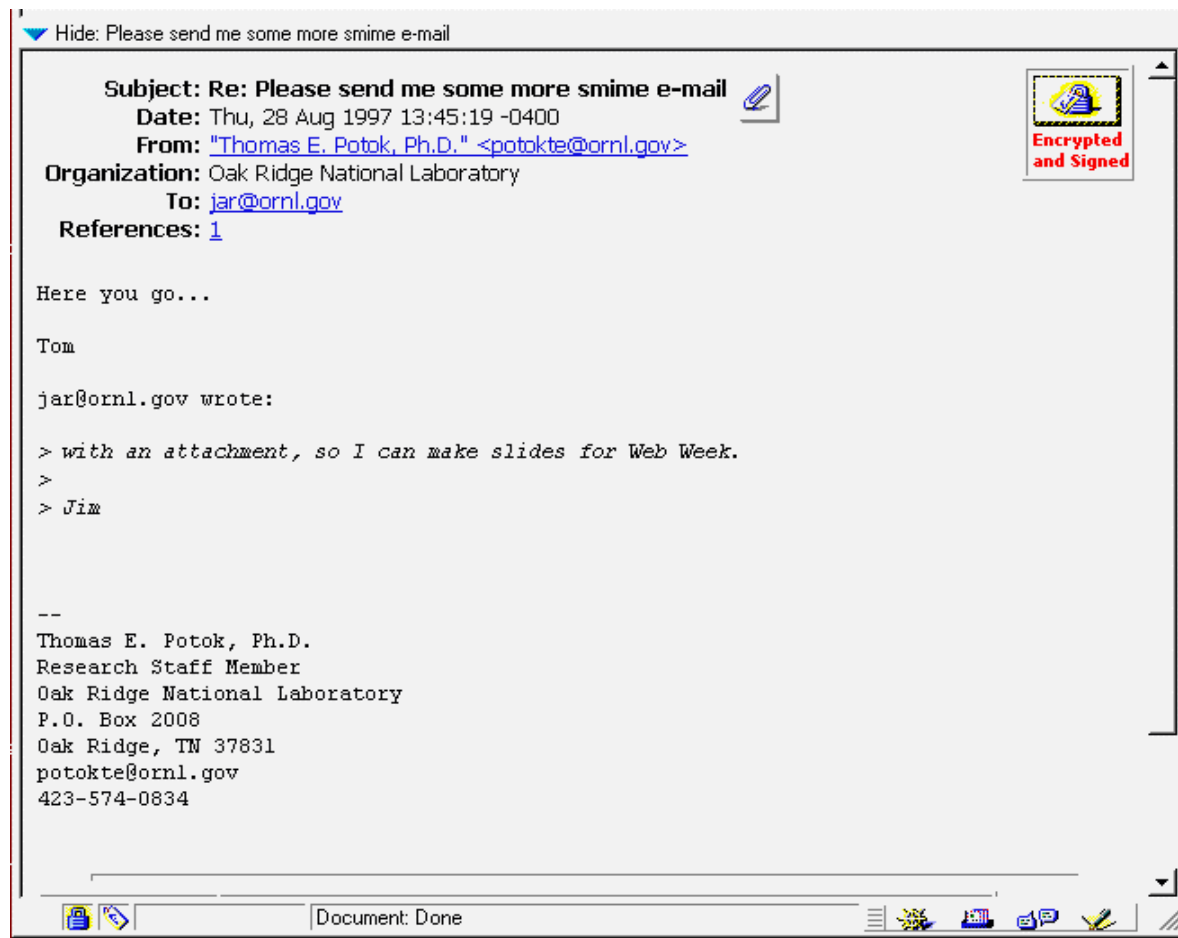
James A. Rome's Materials Microcharacterization Collaboratory ID

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



Certificates also verify downloads


Microsoft Internet Explorer

Authenticode(tm) Security Technology

Do you wish to install and run Authenticode 2.0 Update?

Yes No

Click each link below before relying on this certificate.



Authenticode 2.0 Update
is published by
Microsoft Corporation
as a commercial publisher under credentials issued by
VeriSign Commercial Software Publishers CA

Expires: 5/10/98

In the future, do not show this message for software published by:

Microsoft Corporation

any publisher with credentials from VeriSign Commercial Software Publishers CA

Advanced...

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

The screenshot shows a Netscape browser window with the address bar set to `http://mmc.epm.ornl.gov/dshtml/`. The browser's menu bar includes Certificates, Pubs, Meeting Sites, FileRoom, Web, CIS, Security, Kerberos, NT, My Stuff, LM, MMC, and Lookup. The main content area features a header for "Netscape Directory Server™ 1.02" with a copyright notice for 1996. Below the header is a toolbar with four buttons: Smart Search, Advanced Search, New Entry, and Authentication. The main text area contains a welcome message and a table of tasks.

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 buttons to 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 selects one or 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 what type 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 your directory, you may need to be granted special permission to add new entries. If you are not sure, ask your system administrator. |
| Authenticate | You use the authentication screens to log into and out of the directory. You need to authenticate before you can modify or add entries to the directory. You may also need to authenticate before searching the directory, if your system administrator requires it. |

Document: Done

Accessing an LDAP in Netscape

You can import a new LDAP server into Netscape:

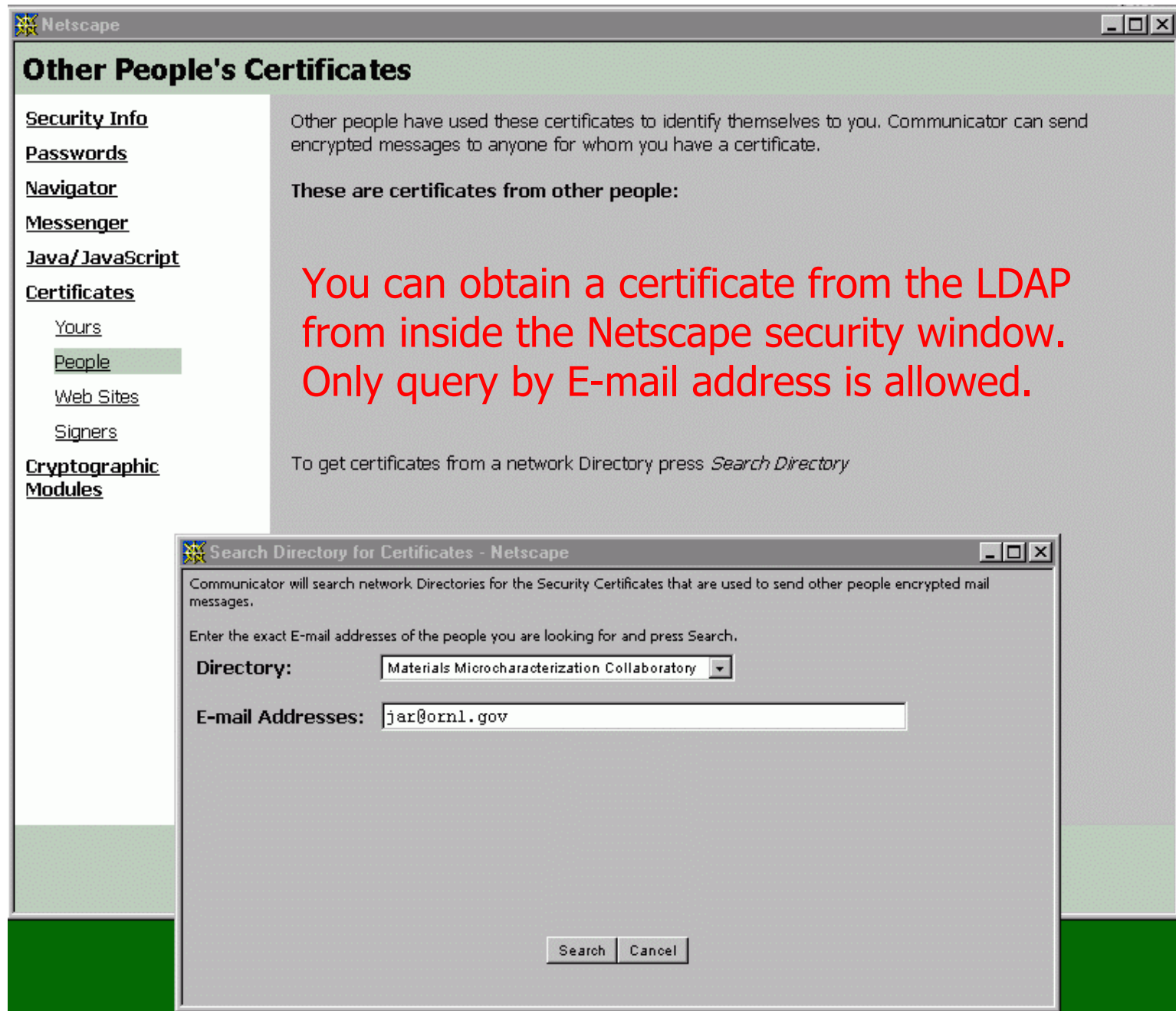
⌘ For my LDAP, access the following URL:

`ldap://mmc.epm.ornl.gov:389/o%3DMaterials%20Microcharacterization%20Collaboratory%2C%20c%3DUS`

⌘ The complicated argument specifies the LDAP root hierarchy.

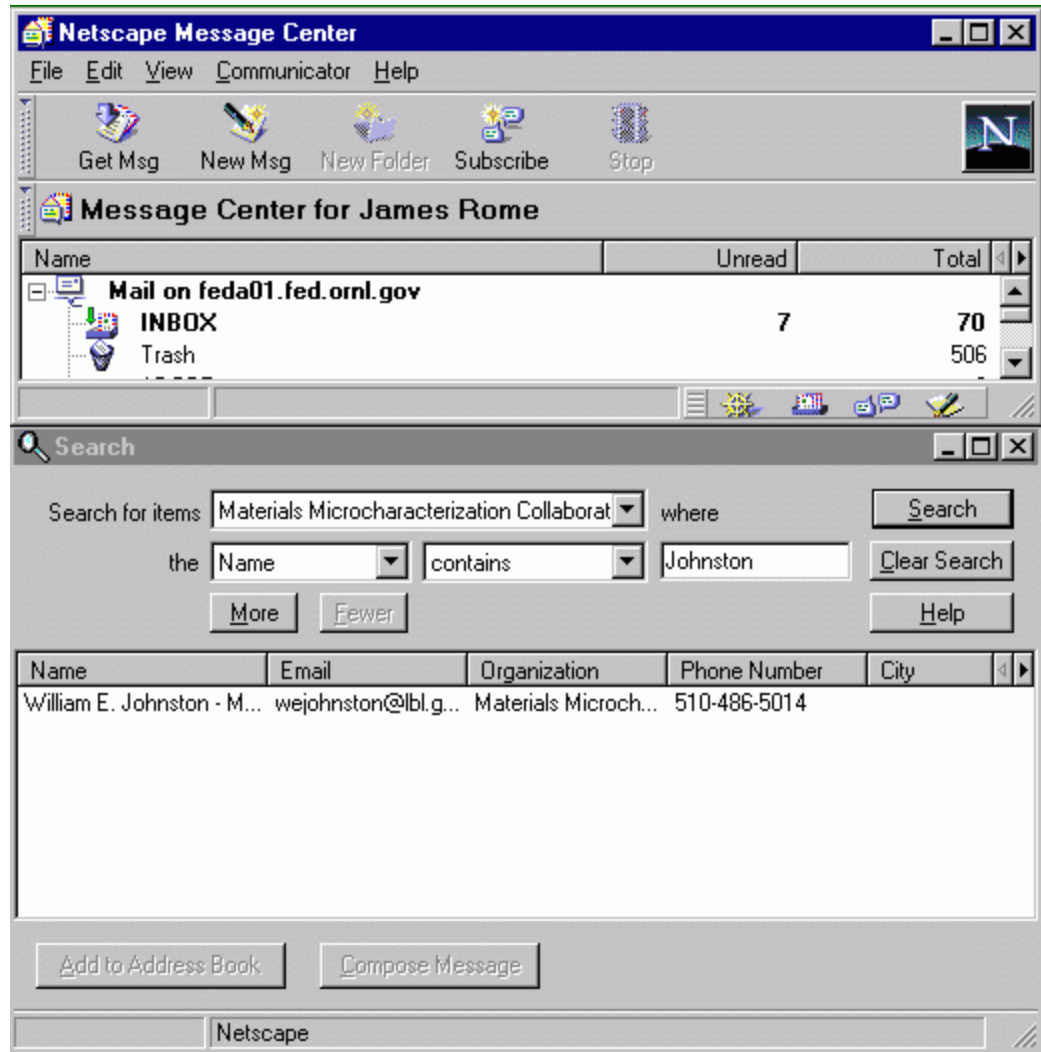
- ◆ All MMC DNs have C=US, O=Materials Microcharacterization Collaboratory

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



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...