United States
Nuclear Regulatory Commission

NRC Electronic Information Exchange (EIE) Instructional Guide

DRAFT

Office of the Chief Information Officer
Information Management Division

May 22, 2000

Prepared under:

Prime Contract No. GS 35F-4813G
Work Order No. T0698BN1516
Modification: 8MJ021SN1/PC04

Prepared by:

LABAT
LABAT-ANDERSON INCORPORATED
8000 Westpark Drive, Suite 400
McLean, Virginia 22102 • 703-506-9600

TABLE OF CONTENTS

1.0 INTRODUCTION
- 1.1 Background 1-1
- 1.2 EIE Business Description 1-1
- 1.3 Who Can Participate 1-2
- 1.4 How to Register 1-2
- 1.5 What is Needed to Participate 1-2

2.0 SETUP TO USE EIE SYSTEM
- 2.1 Introduction 2-1
- 2.2 How to Obtain a Digital ID Certificate 2-1
- 2.3 Establishing Private Key Security 2-7
- 2.4 Approving the Digital ID Certificate 2-10
- 2.5 Retrieving and Installing the Digital ID Certificate 2-11
- 2.6 Verifying Successful Installation 2-13
- 2.7 Obtaining the Netscape Signaturing File 2-16
- 2.8 Obtaining the InternetForm Viewer 2-20
- 2.9 Providing Backup for Digital ID Certificates 2-25
- 2.10 Replacing Digital ID Certificates 2-29
- 2.11 Replacing Netscape Digital ID Certificate Passwords 2-31

3.0 HOW TO SUBMIT DOCUMENTS
- 3.1 EIE Document Submission/Transmission 3-1
- 3.2 How to Obtain the NRC EIE Form 3-1
- 3.3 How to Complete the Form 3-4
- 3.4 How to Enclose Documents 3-6
- 3.5 How to Sign (or Unsign) Documents 3-7
- 3.6 How to Submit/Transmit Documents 3-11
- 3.7 How to Remove Documents 3-13

4.0 HOW TO RETRIEVE DOCUMENTS
- 4.1 Introduction 4-1
- 4.2 How to Search for Documents 4-1
- 4.3 Authenticating the Form and Validating the Signature 4-6
- 4.4 Document Access and Retrieval 4-8
- 4.5 Deleting and Saving Forms 4-11

Statement of Liability . . . . a – i

Glossary of Terms . . . . b – i

Appendix A: Digital Certificate Request Confirmation . . . . c – i

Appendix B: Digital ID Certificate Request Disapproval . . . . c – ii

Appendix C: Digital ID Certificate Approval Notification . . . . c – iii

1.0 INTRODUCTION

1.1 Background

The Agencywide Documents Access and Management System (ADAMS) has been developed to be the NRC's electronic document and records management system. An integral part of ADAMS is the capability to process and disseminate electronic documents that are either received into the Agency or are created within the Agency. The process providing this capability is called Electronic Information Exchange (EIE). EIE allows both users internal to NRC as well as those external to NRC to exchange electronic documents in a secure and valid manner via the Internet.

The development and use of EIE in the NRC environment are intended to address the mandate of the Government Paperwork Elimination Act, Title XVII of Public Law 105-277, that provides for Federal agencies, by October 21, 2003, to give persons who are required to maintain, submit, or disclose information the option of doing so electronically. It is also intended to provide for the use of electronic authentication (electronic signature) methods to verify the identity of the sender and the integrity of electronic content where necessary. The Act specifically provides that electronic records and their related electronic signatures are not to be denied legal effect, validity, or enforceability merely because they are in electronic form.

The NRC is in the implementation stage of the NRC EIE program. The objective of the program is to institute business processes that enable the NRC and the customers and clients of the NRC to interact and communicate electronically in a secure manner via the Internet. In addition, the objective is to document and preserve electronic submissions and transmissions in a manner consistent with that for paper documents. Finally, this undertaking is expected to provide the basis for further evaluation and analysis enabling operational and procedural improvements to the EIE process prior to Agency-wide implementation.

1.2 EIE Business Description

The NRC EIE system design is based on a public key infrastructure (PKI) that provides the capability to exchange electronic documents in a secure manner via the Internet using Secure Sockets Layer (SSL3) technology. In addition, it incorporates the use of digital signature technology to provide submitter (sender) validation and document authentication. The purpose of this document is to provide instructions for participation in the EIE Program.

1.3 Who Can Participate

The participant population includes the NRC and its customers and clients who choose to electronically submit regulatory required submittals in compliance with 10 CFR Part 50.4. The participants internal to the NRC will include offices whose customers and clients choose the EIE process to submit documents electronically in a secure and valid manner via the Internet. The offices will designate individual users who have the responsibility for originating, signing, or receiving official submittals into the Agency. Participants external to the NRC will include those individuals designated having the responsibility of originating, signing, or sending documents to the NRC in compliance with 10 CFR Part 50.4.

1.4 How to Register

The NRC provides for overall administration of the EIE process through the designated Local Registration Authority Administrator (LRAA). The LRAA creates and maintains an Access Control List (ACL) consisting of authorized internal and external EIE participants. Each participant will provide the LRAA with vital information such as name, organization name, phone number, and e-mail address. The LRAA will verify participant information (via e-mail) before adding them to the ACL. The information provided to the LRAA is entered into a secure database and is used to create and distribute secure account information for access to the NRC EIE external server for the dissemination of electronic documents. It is important that participants review this information and make all necessary corrections or additions. The LRAA will use the ACL to validate authorized individuals requesting digital signature certificates. The LRAA may be contacted via e-mail at LRAA@nrc.gov.

1.5 What is Needed to Participate

Participating individuals in the EIE initiative may use their existing workstations with standard desktop configuration. The recommended workstation configuration requires a Pentium 133 Mhz (or higher) with a minimum of 32 MB of RAM, 20 MB of available disk space, and access to the World Wide Web (web) through an Internet Service Provider (ISP). The operating system should be either Windows NT or Windows 95 (or higher). In addition, each workstation must be equipped with browser software consisting of either Netscape Navigator or Communicator (version 4.6 or higher) or Microsoft Internet Explorer (version 5.0). Other browser types such as AOL or Mosaic are not currently supported for use in the EIE process. All other software needed in the EIE process will be available via the NRC EIE external server home page or designated URLs. Listed below are the specific software plug-ins required, their file names, and the URLs where they can be obtained.

Software/Plug-ins	File Name	Location (Download from)
InternetForm Viewer (Browser Application)	IFV431G.EXE	www.nrc.gov/NRC/EIE/index.html (Step 1)
Netscape 4.x plug-in (signaturing piece)	IFXNDSS.EXE	www.nrc.gov/NRC/EIE/index.html (Step 2)
Microsoft Internet Explorer 4.x plug-in (viewer patch)	MASQ_URL.EXE	www.nrc.gov/NRC/EIE/index.html (Step 2)
Digital ID Certificate		www.nrc.gov/NRC/EIE/index.html (Step 3)

Table 1-1: Required Software

2.0 HOW TO START USING EIE SYSTEM

2.1 Introduction

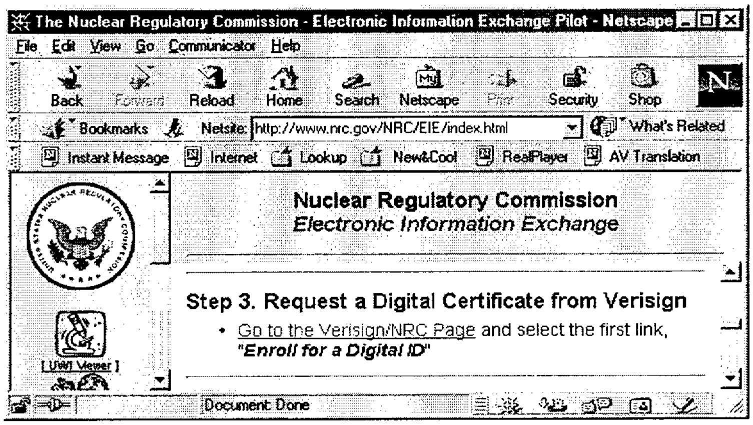
In order to utilize EIE, each individual must obtain a digital signature certificate (Digital ID). Additionally, each of the software plug-ins listed above in Table 1-1 must be downloaded and installed. In the succeeding sections, each process and step required to set-up a computer or workstation to use EIE is described. The processes and steps described are specific to both Netscape Navigator/Communicator 4.6 or higher and Microsoft Internet Explorer 5.0.

2.2 How to Obtain a Digital ID Certificate

All users must have a digital signature certificate (Digital ID) in order to use EIE. (Refer to the Glossary of Terms for a full description of a Digital ID certificate.) A Digital ID is used to digitally sign the form used to submit documents and is required in order to access the EIE external server and retrieve documents. The EIE system requires the use of an NRC issued Digital ID.

To obtain a Digital ID, authorized participants (applicants) must first complete and submit an enrollment form. VeriSign, Inc. acts as the NRC's Certificate Authority (CA) and provides the NRC with a Digital ID enrollment page on their web site. The NRC provides VeriSign Onsite Digital ID's at no cost. The steps for obtaining a Digital ID are as follows:

Step 1: Applicants can apply for a Digital ID by accessing the EIE home page at www.nrc.gov/NRC/EIE/index.html . When the NRC EIE home page appears, go to Step 3 (on EIE home page). **Click on Go to the VeriSign/NRC Page.**


The Nuclear Regulatory Commission - Electronic Information Exchange Pilot - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop
Bookmarks Netsite:
What's Related
Instant Message Internet Lookup New&Cool RealPlayer AV Translation
[UWI Viewer]
Document: Done

http://www.nrc.gov/NRC/EIE/index.html

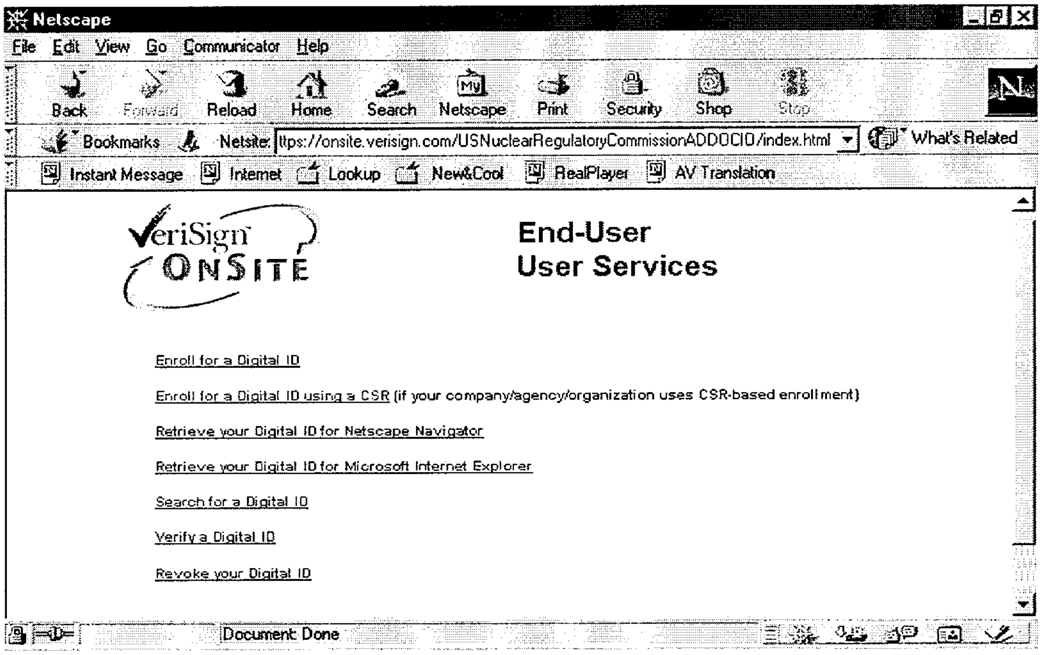
Nuclear Regulatory Commission
Electronic Information Exchange

Step 3. Request a Digital Certificate from Verisign

- Go to the Verisign/NRC Page and select the first link, ***"Enroll for a Digital ID"***

Figure 2-1: EIE Home Page

Step 2: Once connected, the VeriSign Onsite End-User User Services page appears at (https://onsite.verisign.com/USNuclearRegulatoryCommissionADDOCIO/index.html). Applicants begin the enrollment process by selecting the first option presented, "Enroll for a Digital ID."


Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Netsite: ttps://onsite.verisign.com/USNuclearRegulatoryCommissionADDOCIO/index.html
What's Related
Instant Message Internet Lookup New&Cool RealPlayer AV Translation
VeriSign OnSite
Document: Done

End-User
User Services

Enroll for a Digital ID

Enroll for a Digital ID using a CSR (if your company/agency/organization uses CSR-based enrollment)

Retrieve your Digital ID for Netscape Navigator

Retrieve your Digital ID for Microsoft Internet Explorer

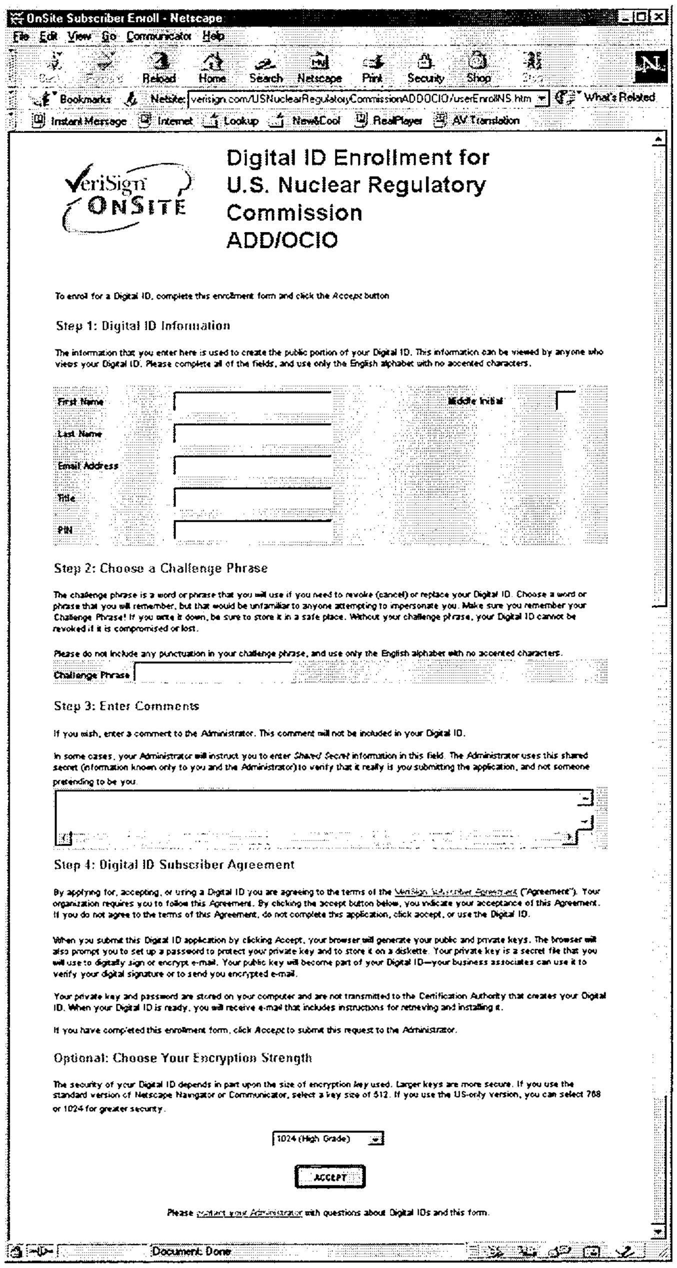
Search for a Digital ID

Verify a Digital ID

Revoke your Digital ID

Figure 2-2: NRC VeriSign Onsite Enrollment Page

After selecting this option, the applicant is presented with an online enrollment form. When enrolling, applicants must use the same computer on which they intend to install the Digital ID and private key.



Digital ID Enrollment for U.S. Nuclear Regulatory Commission ADD/OCIO

To enrol for a Digital ID, complete this enrollment form and click the *Accept* button

Step 1: Digital ID Information

The information that you enter here is used to create the public portion of your Digital ID. This information can be viewed by anyone who views your Digital ID. Please complete all of the fields, and use only the English alphabet with no accented characters.

First Name		Middle Initial	
Last Name			
Email Address			
Title			
PIN			

Step 2: Choose a Challenge Phrase

The challenge phrase is a word or phrase that you will use if you need to revoke (cancel) or replace your Digital ID. Choose a word or phrase that you will remember, but that would be unfamiliar to anyone attempting to impersonate you. Make sure you remember your Challenge Phrase! If you write it down, be sure to store it in a safe place. Without your challenge phrase, your Digital ID cannot be revoked if it is compromised or lost.

Please do not include any punctuation in your challenge phrase, and use only the English alphabet with no accented characters.

Challenge Phrase

Step 3: Enter Comments

If you wish, enter a comment to the Administrator. This comment will not be included in your Digital ID.

In some cases, your Administrator will instruct you to enter *Shared Secret* information in this field. The Administrator uses this shared secret (information known only to you and the Administrator) to verify that it really is *you* submitting the application, and not someone pretending to be you.

Step 4: Digital ID Subscriber Agreement

By applying for, accepting, or using a Digital ID you are agreeing to the terms of the VeriSign Subscriber Agreement ("Agreement"). Your organization requires you to follow this Agreement. By clicking the accept button below, you indicate your acceptance of this Agreement. If you do not agree to the terms of this Agreement, do not complete this application, click accept, or use the Digital ID.

When you submit this Digital ID application by clicking Accept, your browser will generate your public and private keys. The browser will also prompt you to set up a password to protect your private key and to store it on a diskette. Your private key is a secret file that you will use to digitally sign or encrypt e-mail. Your public key will become part of your Digital ID—your business associates can use it to verify your digital signature or to send you encrypted e-mail.

Your private key and password are stored on your computer and are not transmitted to the Certification Authority that creates your Digital ID. When your Digital ID is ready, you will receive e-mail that includes instructions for retrieving and installing it.

If you have completed this enrollment form, click *Accept* to submit this request to the Administrator.

Optional: Choose Your Encryption Strength

The security of your Digital ID depends in part upon the size of encryption key used. Larger keys are more secure. If you use the standard version of Netscape Navigator or Communicator, select a key size of 512. If you use the US-only version, you can select 768 or 1024 for greater security.

1024 (High Grade)

ACCEPT

Please contact your Administrator with questions about Digital IDs and this form.

Step 3: The form is divided into five parts. Applicants must complete all required information on the enrollment form as follows:

1. **Digital ID Information** - Applicants must complete the first name, middle initial, last name, e-mail address, and title fields. Applicants will be prompted to enter the e-mail address twice to confirm it. The PIN field is not required for enrollment.

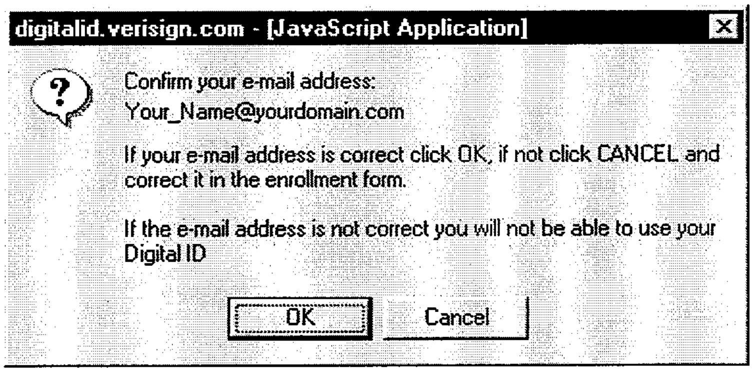
2. **Choose a Challenge Phrase** - Applicants must enter a word or phrase that serves to validate their identity should a situation arise that requires the Digital ID to be canceled or revoked.

3. **Enter Comments** - This part is optional.

4. **Digital ID Subscriber Agreement** - Each applicant is encouraged to read and understand the subscriber agreement.

5. **Choose your Encryption Strength** - Encryption strength refers to the security of the Digital ID. The longer the encryption key the more secure the Digital ID. It is recommended that applicants select the largest key size that can be handled by your browser. (Older browser versions will default to 512 bit keys whereas newer browser versions can handle up to 1024 bit keys.)

Step 4: Submit the enrollment form by clicking on the **Accept** button. You will receive a prompt to make certain your e-mail address is correct. Follow the instructions on the dialog box and click on the **OK** button.


digitalid.verisign.com - [JavaScript Application]

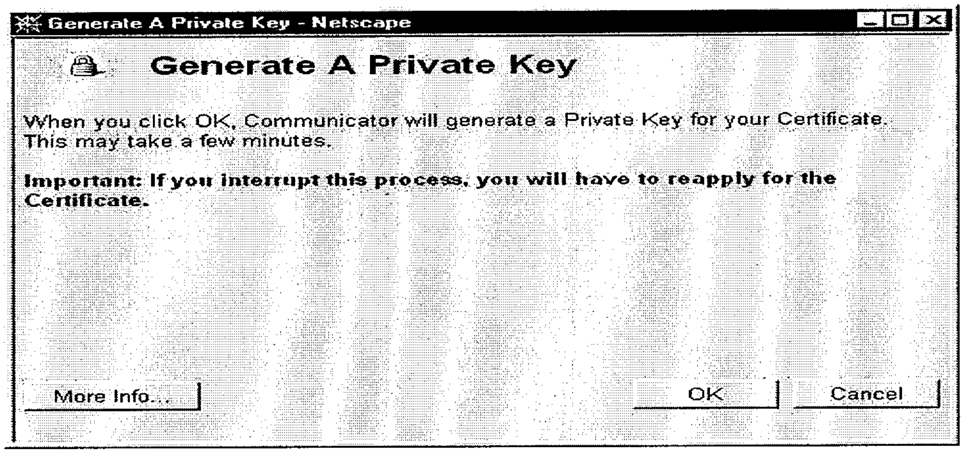
Confirm your e-mail address:
Your_Name@yourdomain.com

If your e-mail address is correct click OK, if not click CANCEL and correct it in the enrollment form.

If the e-mail address is not correct you will not be able to use your Digital ID

Figure 2-4: E-mail Address Confirmation

Step 5: Upon submission of the enrollment form, the applicant is prompted to initiate the generation of the private key as illustrated below. Click on the **OK** button.


Generate A Private Key - Netscape

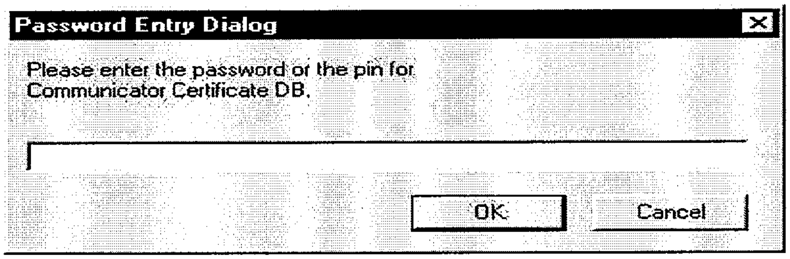
Generate A Private Key

When you click OK, Communicator will generate a Private Key for your Certificate. This may take a few minutes.

Important: If you interrupt this process, you will have to reapply for the Certificate.

Figure 2-5: Generate a Private Key

After clicking on the **OK** button, users of Netscape browsers will be prompted to enter a password for the Certificate Database.

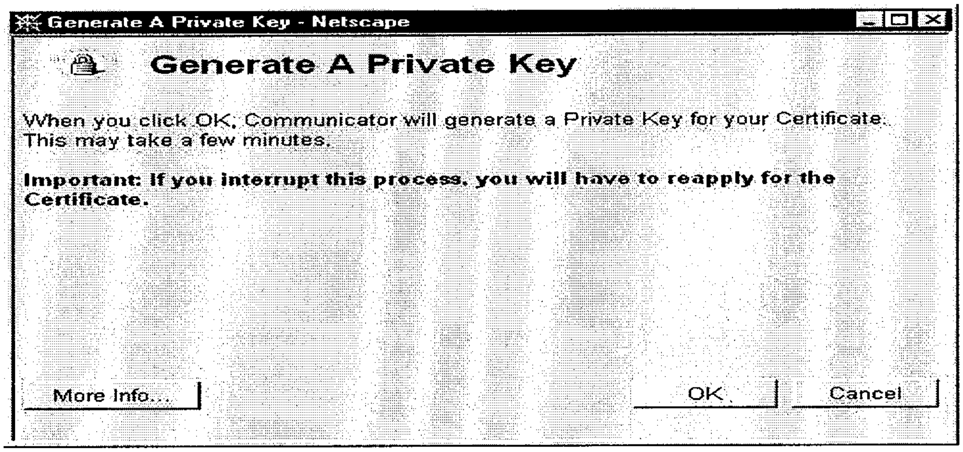

Password Entry Dialog

Please enter the password or the pin for Communicator Certificate DB.

Figure 2-6: Netscape Password Entry Dialog

Step 6: Enter a unique password and click on the **OK** button. You will be prompted to re-enter it for confirmation. (Note: Be sure to choose a password that is easy to remember, yet secure. This is a must since the access to and use of your Digital ID will depend on this password. If you must, write the password down and keep it in a safe place.)

Once the Certificate Database password is entered and confirmed, the Netscape user is returned to the Generate a Private Key dialog.



Generate A Private Key

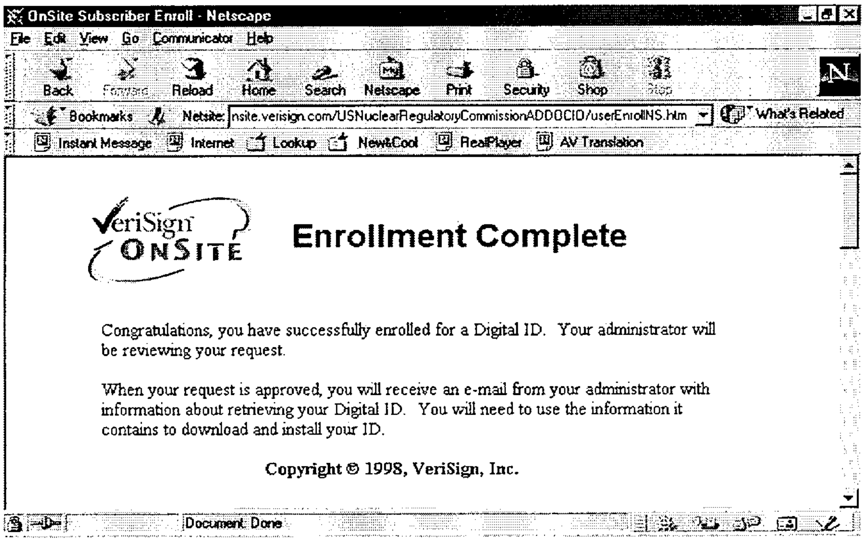
When you click OK, Communicator will generate a Private Key for your Certificate. This may take a few minutes.

Important: If you interrupt this process, you will have to reapply for the Certificate.

Figure 2-7: Generate a Private Key

Step 7: Click on the **OK** button to generate a key. A private key is automatically generated and stored in the browser.

This completes the enrollment process. A window appears stating the enrollment is complete and that the LRAA will review their enrollment application and notify them of the results by e-mail.


OnSite Subscriber Enroll - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Netsite: onsite.verisign.com/USNuclearRegulatoryCommissionADDOCIO/userEnrollNS.htm
What's Related
Instant Message Internet Lookup New&Cool RealPlayer AV Translation
VeriSign OnSite
Document: Done

Enrollment Complete

Congratulations, you have successfully enrolled for a Digital ID. Your administrator will be reviewing your request.

When your request is approved, you will receive an e-mail from your administrator with information about retrieving your Digital ID. You will need to use the information it contains to download and install your ID.

Copyright © 1998, VeriSign, Inc.

Figure 2-8: Enrollment Complete

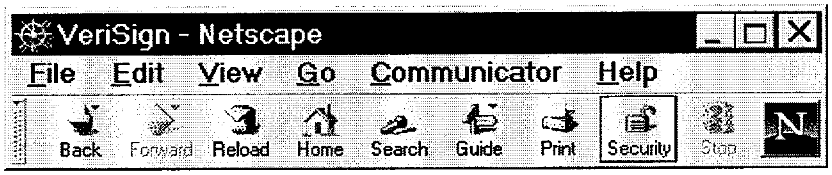
2.3 Establishing Private Key Security

Both Netscape Navigator/Communicator and Microsoft Internet Explorer users can establish password security to protect their private key. The steps applicable to each are outlined below.

Netscape Navigator/Communicator (version 4.6 or higher)

In the case of Netscape, the private key is stored in the Certificate Database which is password protected. The Certificate Database is established during the generation of the private key. (See Section 2.2). You may, however, change your password. This is accomplished as follows.

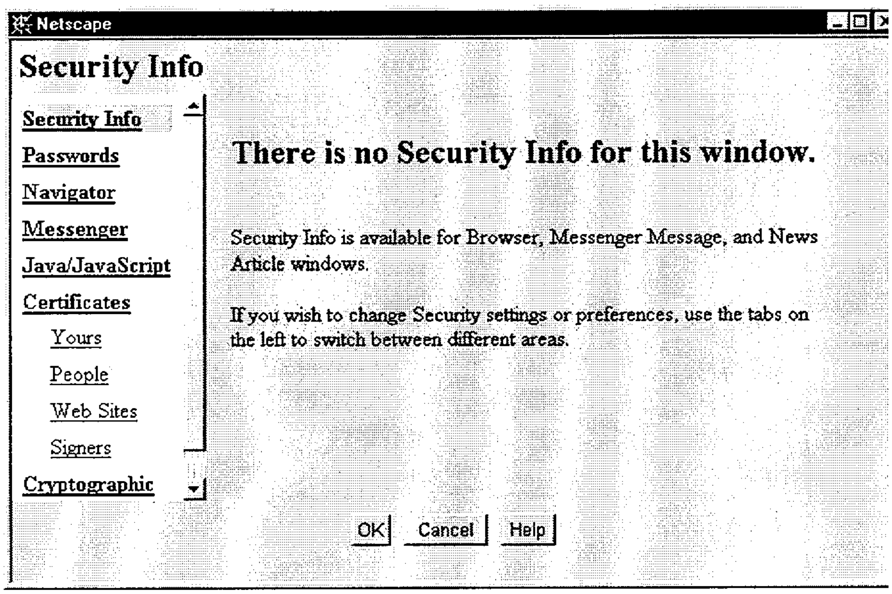
Step 1: Click on the **Security** icon on the Netscape toolbar.



VeriSign - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Guide Print Security Stop

Figure 2-9: Netscape Toolbar

The Security Info window appears.



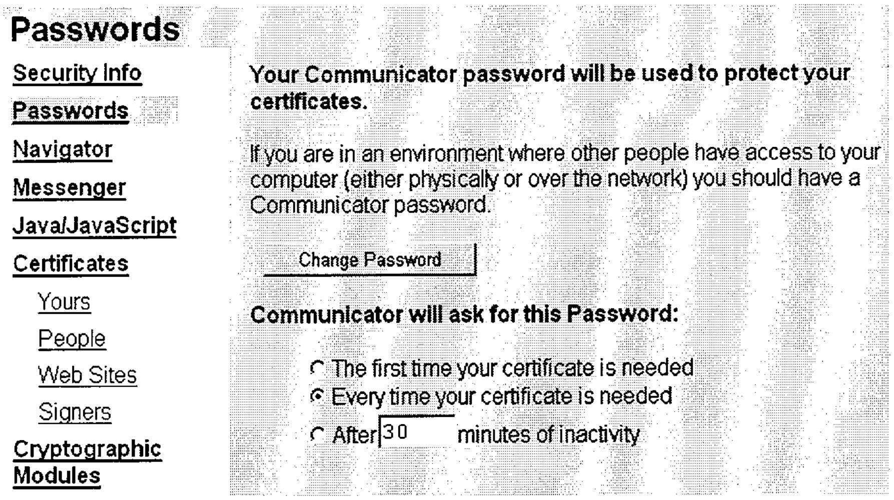
There is no Security Info for this window.

Security Info is available for Browser, Messenger Message, and News Article windows.

If you wish to change Security settings or preferences, use the tabs on the left to switch between different areas.

Figure 2-10: Security Info Window

Step 2: Click on **Passwords**. This invokes the Netscape Passwords window.



Your Communicator password will be used to protect your certificates.

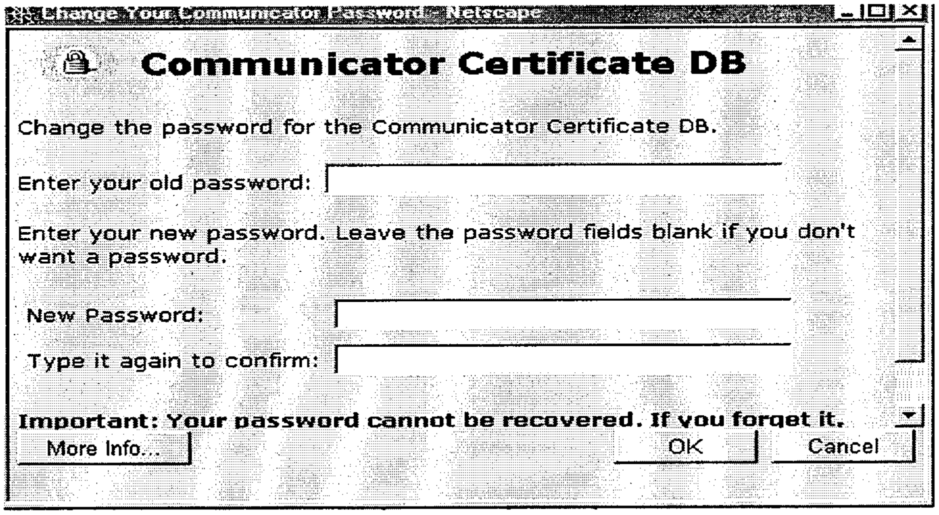
If you are in an environment where other people have access to your computer (either physically or over the network) you should have a Communicator password.

Communicator will ask for this Password:

○ The first time your certificate is needed
● Every time your certificate is needed
○ After 30 minutes of inactivity

Figure 2-11: Netscape Passwords Window

Step 3: Click on the **Change Password** button. This produces the Certificate Database (DB) password entry dialog.


Change Your Communicator Password - Netscape
Communicator Certificate DB
More Info...
OK
Cancel

Change the password for the Communicator Certificate DB.

Enter your old password:

Enter your new password. Leave the password fields blank if you don't want a password.

New Password:

Type it again to confirm:

Important: Your password cannot be recovered. If you forget it,

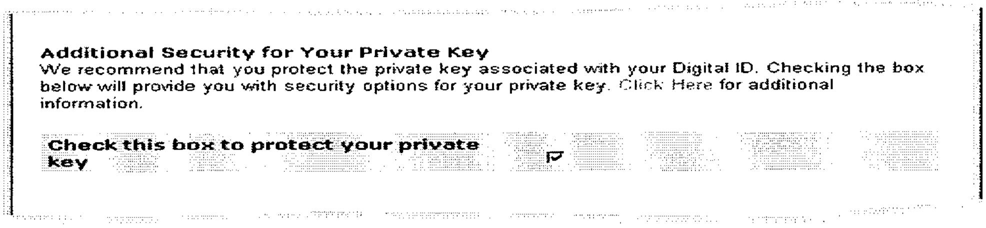
Figure 2-12: Netscape Certificate Database Password Entry

Step 4: Enter your old password. Then enter a unique password and re-enter it to confirm it. Then click on the **OK** button. This establishes a password protected Certificate Database. (Note: Be sure to choose a password that is easy to remember, yet secure. This is a must since the access to and use of your Digital ID will depend on this password. If you must, write the password down and keep it in a safe place.)

Microsoft Internet Explorer (version 5.0 or higher)

Microsoft Internet Explorer users will be allowed to assign additional security to their private key when enrolling for a Digital ID.

Step 1: After clicking to generate a private key, the Additional Security dialog box appears.



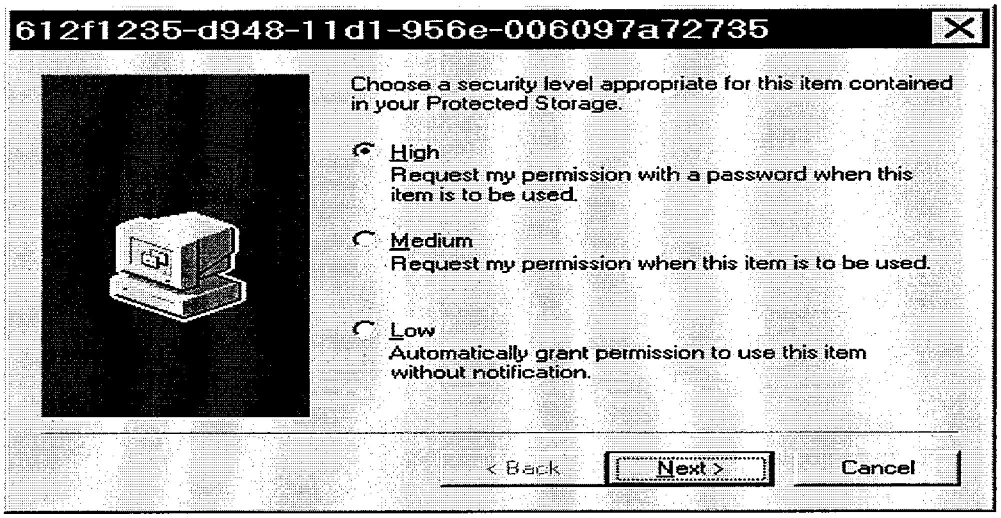
Additional Security for Your Private Key

We recommend that you protect the private key associated with your Digital ID. Checking the box below will provide you with security options for your private key. Click Here for additional information.

Check this box to protect your private key ☑

Figure 2-13: Microsoft Additional Security Dialog

Step 2: If you do not check the box, a private key will be generated. However, if you desire additional security for your private key, place the cursor in the box and click to check the box. In so doing, you will be prompted to choose an appropriate security level. The three security levels - high, medium, or low - are described below.



612f1235-d948-11d1-956e-006097a72735

Choose a security level appropriate for this item contained in your Protected Storage.

● High
Request my permission with a password when this item is to be used.

○ Medium
Request my permission when this item is to be used.

○ Low
Automatically grant permission to use this item without notification.

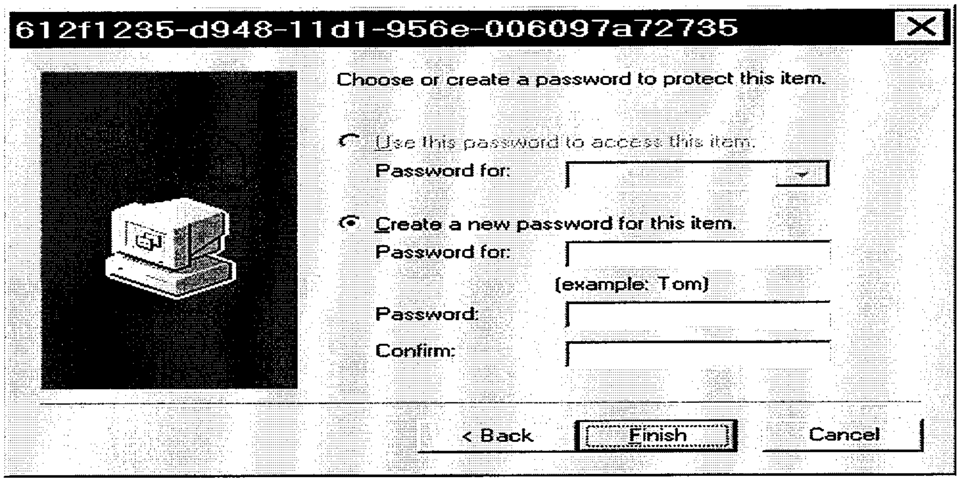
Figure 2-14: Microsoft Security Level Window

High - Requires you to enter a password before your private key is accessed.

Medium - Alerts you and asks for permission before your private key is accessed.

Low - Does not add any additional security. Your private key is protected only by your system's logon procedure.

If you select the "high" security option, you will be prompted to assign a password.



612f1235-d948-11d1-956e-006097a72735

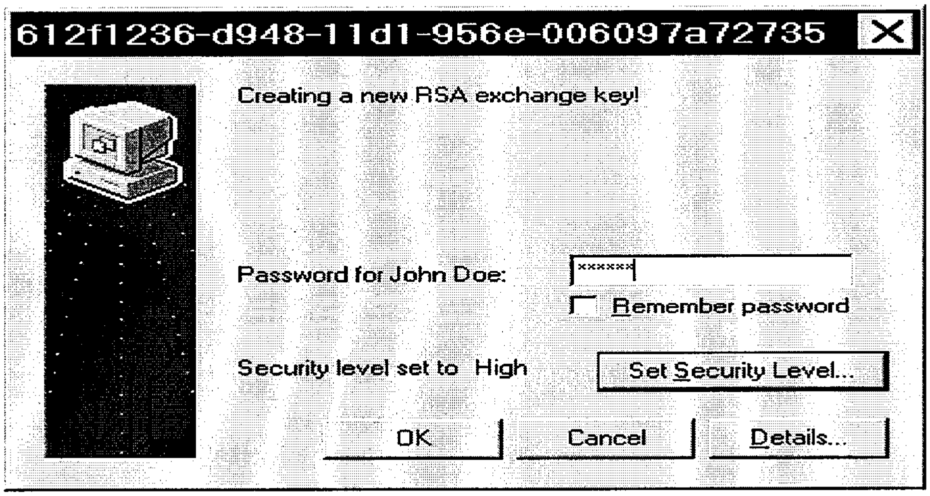
Choose or create a password to protect this item.

○ Use this password to access this item.
Password for:

● Create a new password for this item.
Password for:
(example: Tom)
Password:
Confirm:

Figure 2-15: Microsoft Password Entry

Step 3: After entering and confirming the password, click the **Finish** button. A final window appears asking for the password and allowing the generation of the private key by clicking on the **OK** button.



612f1236-d948-11d1-956e-006097a72735

Creating a new RSA exchange key!

Password for John Doe: ******

□ Remember password

Security level set to High

Figure 2-16: Microsoft High Security

2.4 Approving the Digital ID Certificate

The Digital ID enrollment form is transmitted to the LRAA via a secure link using SSL3. When the form is submitted to the LRAA, an e-mail message is generated and sent to the applicant acknowledging it's receipt. (See Appendix A.) The LRAA validates the information contained in the form using the ACL. If the information matches that in the

ACL, the LRAA approves the issuance of a Digital ID certificate. If the information does not match that in the ACL, the LRAA shall deny the issuance of a Digital ID certificate. In either case, an e-mail message is generated to the applicant notifying them of the decision.

Each applicant is expected to be approved unless he or she did not receive authorization or failed to properly register with the LRAA. In the case of a disapproved request, the LRAA will provide e-mail notification of the disapproval and will endeavor to provide a specific reason for it. (See Appendix B.) Once the applicant appropriately addresses the reason for disapproval, a new enrollment form can be submitted. The LRAA shall serve as the point of contact for any questions related to the enrollment process and shall make every effort to process requests for Digital IDs within two business days of receipt.

2.5 Retrieving and Installing the Digital ID Certificate

Upon approval, applicants are notified of the decision via e-mail. The e-mail shall contain instructions on how to access and retrieve the Digital ID certificate. (See Appendix C.) The e-mail instructions shall include the following:

1. Statement of the URL where the digital certificate can be retrieved.

2. The personal identification number (PIN) needed to retrieve the digital certificate, e.g., 892137890.

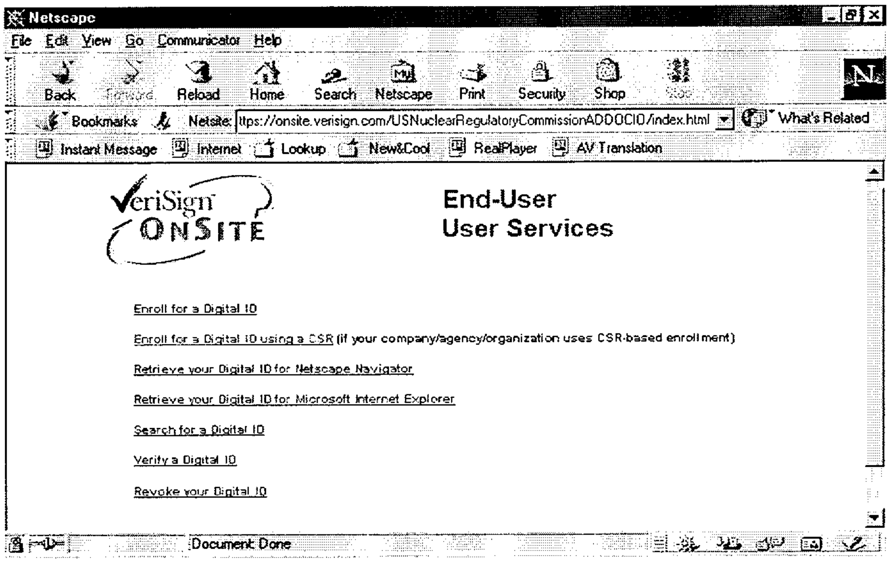
3. Statement to follow instructions on the web page to complete installation of the digital certificate (Digital ID).

To retrieve and install the Digital ID, participants must use the same computer used to submit the enrollment form. To successfully install the Digital ID, follow the steps listed below.

Step 1: With the e-mail open, copy the PIN by highlighting it and pressing the "Ctrl" and "C" keys at the same time or by highlighting it, right clicking with your mouse, and selecting copy from the shortcut menu.

Step 2: Click on the URL provided in the same e-mail message, i.e., (https://onsite.verisign.com/USNuclearRegulatoryCommissionADDOCIO/index.html.)

Step 3: Once connected, the participant is presented with the VeriSign OnSite Host page for NRC.



Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Netsite: ttps://onsite.verisign.com/USNuclearRegulatoryCommissionADDOCIO/index.html What's Related
Instant Message Internet Lookup New&Cool RealPlayer AV Translation
VeriSign OnSite
Document: Done

End-User
User Services

Enroll for a Digital ID

Enroll for a Digital ID using a CSR (if your company/agency/organization uses CSR-based enrollment)

Retrieve your Digital ID for Netscape Navigator

Retrieve your Digital ID for Microsoft Internet Explorer

Search for a Digital ID

Verify a Digital ID

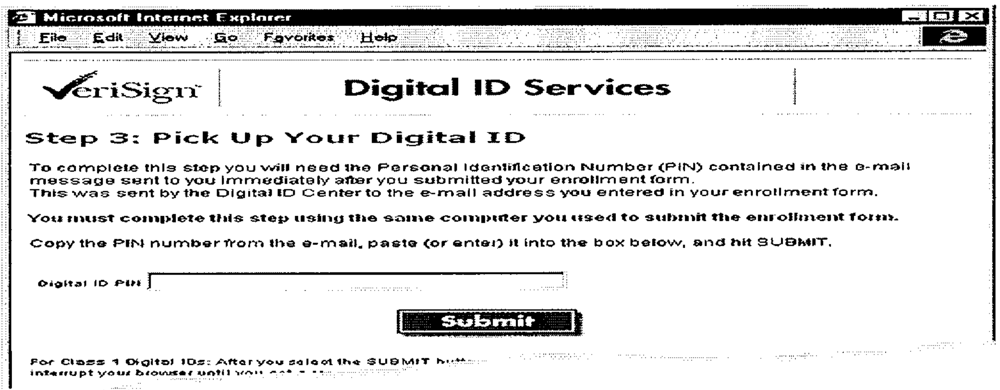
Revoke your Digital ID

Figure 2-17: NRC VeriSign OnSite Host Page

Of the options presented, options 3 and 4 are for retrieval of a Digital ID. Depending on whether your browser is Netscape Navigator/Communicator or Microsoft Internet Explorer, select the appropriate option.

The participant is presented with the VeriSign Digital ID Services window that allows the participant to "Pick up your Digital ID."

Step 4: Paste the **PIN** number provided in the e-mail (and copied in Step 1) in the Digital ID PIN box by clicking your cursor within the box and pressing the "Ctrl" and "V" keys at the same time or right clicking and selecting **Paste** from the shortcut menu.



Digital ID Services

Step 3: Pick Up Your Digital ID

To complete this step you will need the Personal Identification Number (PIN) contained in the e-mail message sent to you immediately after you submitted your enrollment form.
This was sent by the Digital ID Center to the e-mail address you entered in your enrollment form.

You must complete this step using the same computer you used to submit the enrollment form.

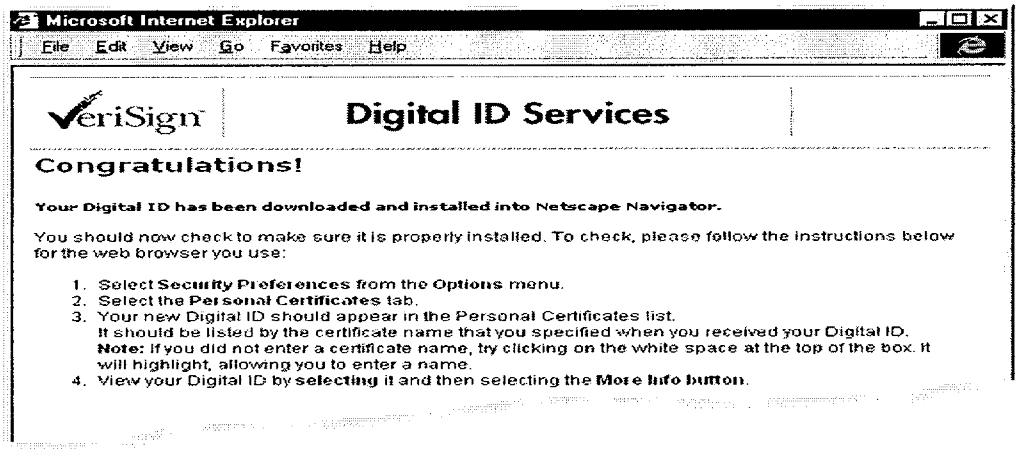
Copy the PIN number from the e-mail, paste (or enter) it into the box below, and hit SUBMIT.

Digital ID PIN

For Class 1 Digital IDs: After you select the SUBMIT
interrupt your browser until

Figure 2-18: Pick Up Your Digital ID

Step 5: Click on **Submit** to install your Digital ID. (Note: Netscape users are prompted to enter their certificates database password before installation proceeds.) When the installation is complete, a Congratulations message will appear indicating a successful download and installation. In addition, it will contain instructions on how to check to ensure proper installation.



Congratulations!

Your Digital ID has been downloaded and installed into Netscape Navigator.

You should now check to make sure it is properly installed. To check, please follow the instructions below for the web browser you use:

1. Select **Security Preferences** from the **Options** menu.
2. Select the **Personal Certificates** tab.
3. Your new Digital ID should appear in the Personal Certificates list.
   It should be listed by the certificate name that you specified when you received your Digital ID.
   Note: If you did not enter a certificate name, try clicking on the white space at the top of the box. It will highlight, allowing you to enter a name.
4. View your Digital ID by **selecting** it and then selecting the **More Info button**.

Figure 2-19: Successful Download and Installation

2.6 Verifying Successful Installation

Once the installation process is complete, the participant is encouraged to check or verify the installation of their Digital ID certificate. The process of verifying installation is similar for both Netscape Navigator/Communicator and Microsoft Internet Explorer users. The steps applicable to each are outlined below.

Netscape Navigator/Communicator (version 4.6 or higher)

Step 1: Click on the **Security** icon on the Netscape toolbar.

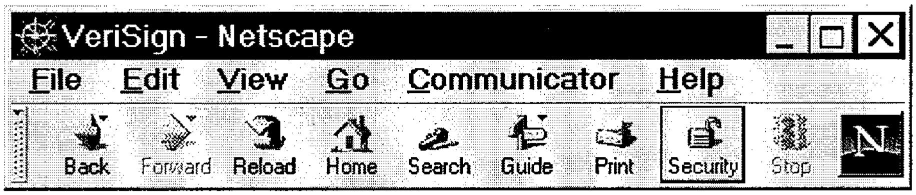
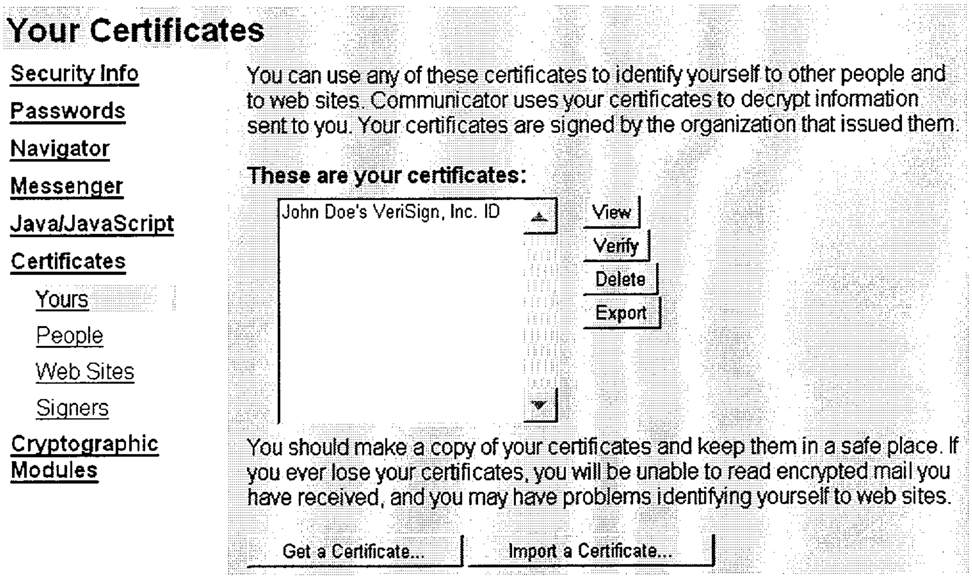


Figure 2-20: Netscape Toolbar Security Icon

Step 2: The Security Advisor/Info window opens. Select <u>**Yours**</u> from the left hand margin under Certificates. Your Digital ID should appear in the "These are your certificates" window. Highlight your Digital ID and click on the **View** button.



Your Certificates

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.

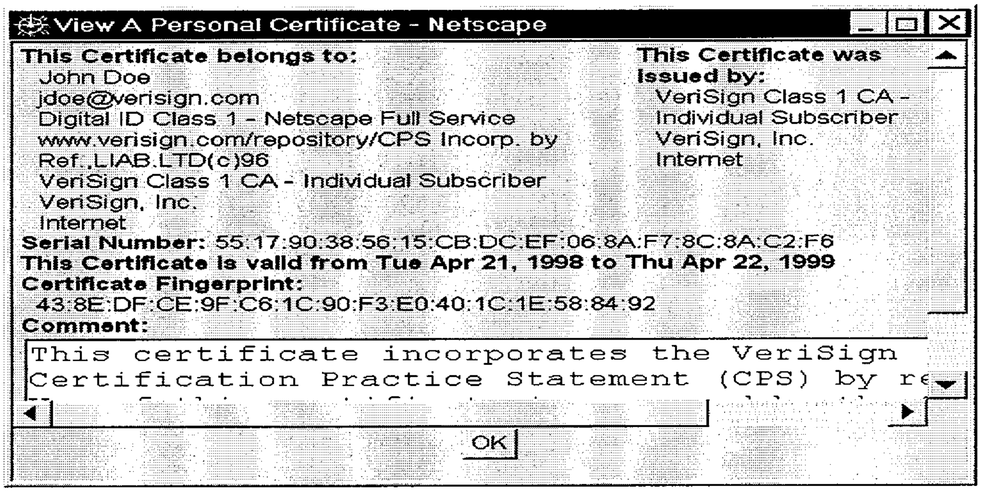
These are your certificates:

John Doe's VeriSign, Inc. ID

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.

Figure 2-21: Your Certificates Window

Step 3: Your Digital ID should appear in the "These are your certificates" window. Highlight your Digital ID and click on the **View** button to display the contents of your Digital ID.



This Certificate belongs to:
John Doe
jdoe@verisign.com
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

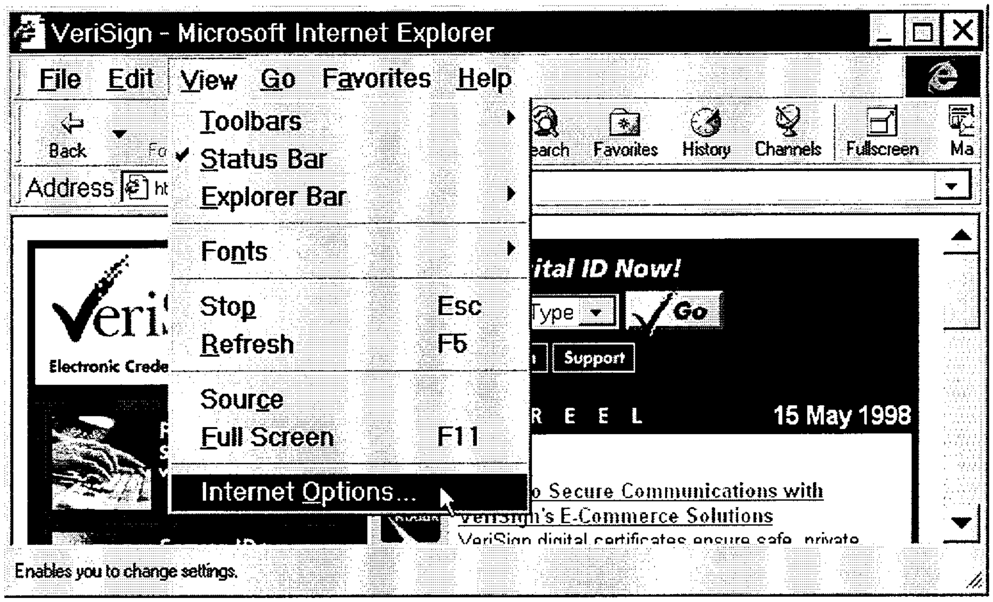
Serial Number: 55:17:90:38:56:15:CB:DC:EF:06:8A:F7:8C:8A:C2:F6
This Certificate is valid from Tue Apr 21, 1998 to Thu Apr 22, 1999
Certificate Fingerprint:
43:8E:DF:CE:9F:C6:1C:90:F3:E0:40:1C:1E:58:84:92
Comment:

```
This certificate incorporates the VeriSign
Certification Practice Statement (CPS) by re
```

Figure 2-22: Personal Certificate

Microsoft Internet Explorer (version 5.0 or higher)

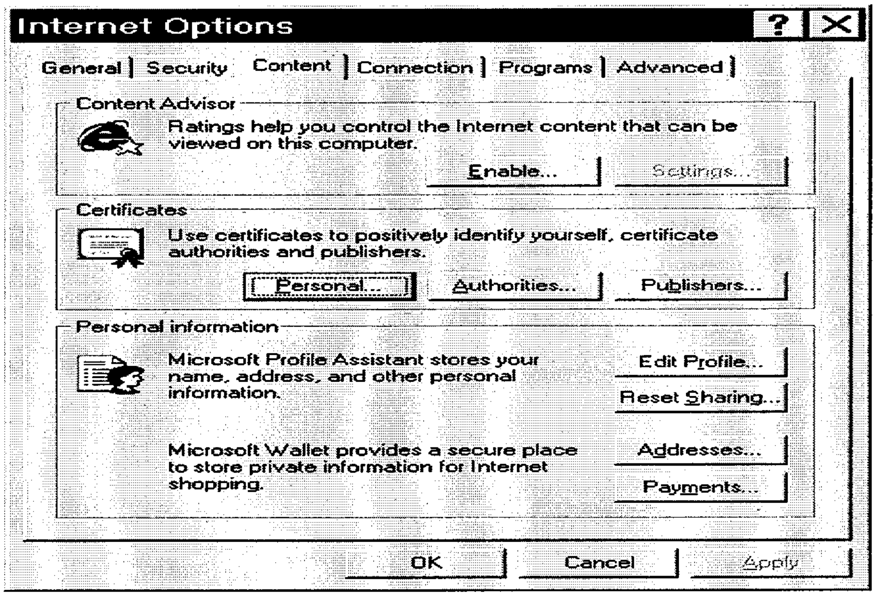
Step 1: Select **View** from the menu bar and click on **Internet Options** on the drop down menu.



Enables you to change settings.

Figure 2-23: Microsoft Internet Explorer Menu Bar and Drop Down

Step 2: In the Internet Options window, click on the **Content** tab, select **Personal**, and click on the **OK** button.



Ratings help you control the Internet content that can be viewed on this computer.

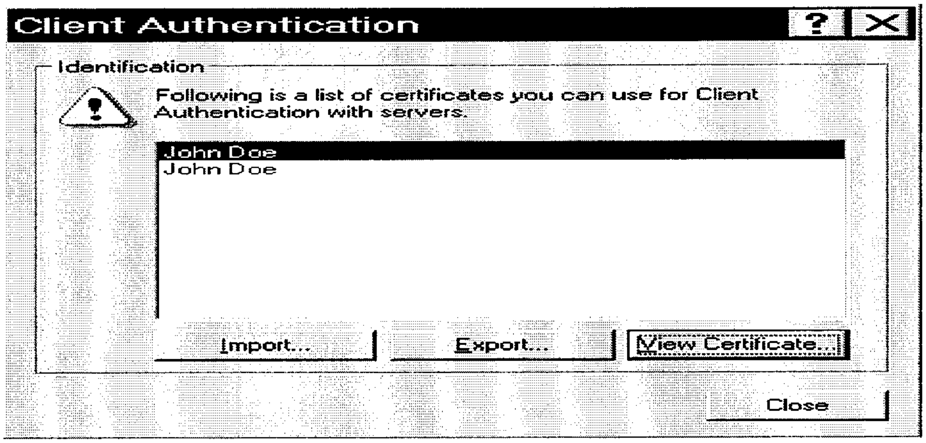
Use certificates to positively identify yourself, certificate authorities and publishers.

Microsoft Profile Assistant stores your name, address, and other personal information.

Microsoft Wallet provides a secure place to store private information for Internet shopping.

Figure 2-24: Internet Options Window

Step 3: The Client Authentication window appears. Highlight your **Digital ID** and click on **View Certificate.**

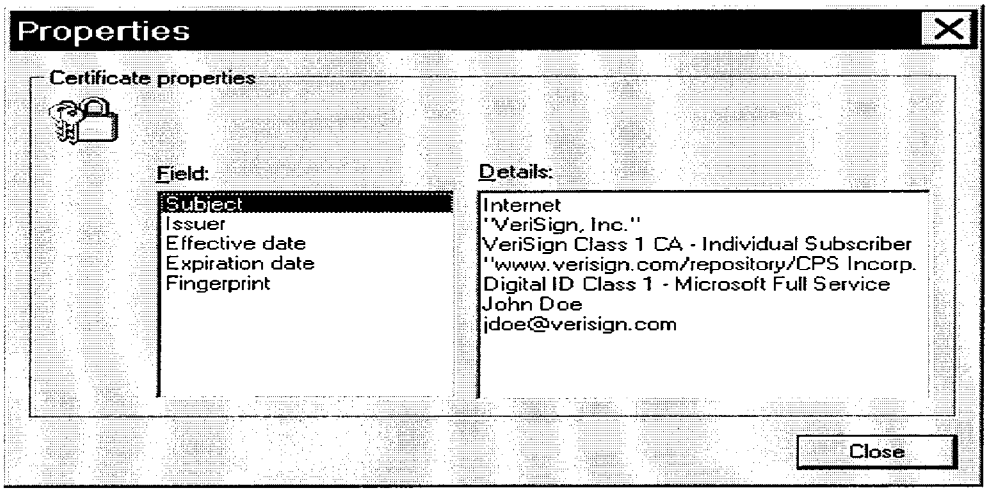


Following is a list of certificates you can use for Client Authentication with servers.

John Doe
John Doe

Figure 2-25: Client Authentication Window

Step 4: View the contents of your Digital ID in the Certificate Properties window that appears.



Field:
Subject
Issuer
Effective date
Expiration date
Fingerprint

Details:
Internet
"VeriSign, Inc."
VeriSign Class 1 CA - Individual Subscriber
"www.verisign.com/repository/CPS Incorp.
Digital ID Class 1 - Microsoft Full Service
John Doe
jdoe@verisign.com

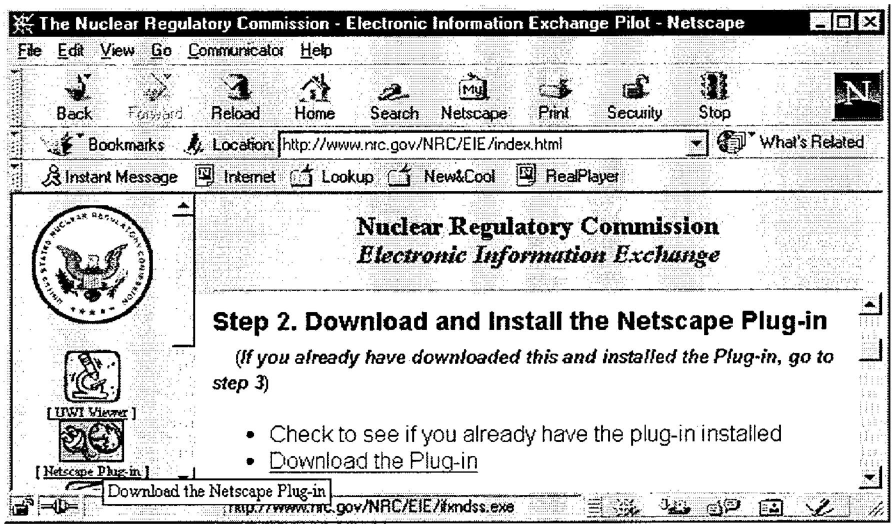
Figure 2-26: Microsoft Certificate Properties Window

If your Digital ID fails to appear as described above, you will need to return to the VeriSign Onsite host page and retrieve your certificate again. (See Section 2.5.) If this subsequent attempt fails, you will need to re-enroll. (See Section 2.2.)

2.7 Obtaining the Netscape Signaturing File

In order to sign or verify signatures, Netscape users will need to obtain a special digital signature file. The required file is named "DS_Netscape.ifx" and can be obtained via the NRC EIE home page. In order to obtain and install the Netscape signaturing file, follow the instructions below.

Step 1: Access the NRC EIE home page at http://www.nrc.gov./NRC/EIE/index.html. Go to Step 2 and click on **Download the Plug-in** to download the Netscape signaturing plug-in for your browser.


The Nuclear Regulatory Commission - Electronic Information Exchange Pilot - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Location: http://www.nrc.gov/NRC/EIE/index.html
What's Related
Instant Message Internet Lookup New&Cool RealPlayer
[IIWI Viewer]
[Netscape Plug-in]
Download the Netscape Plug-in
http://www.nrc.gov/NRC/EIE/ifxndss.exe

Nuclear Regulatory Commission
Electronic Information Exchange

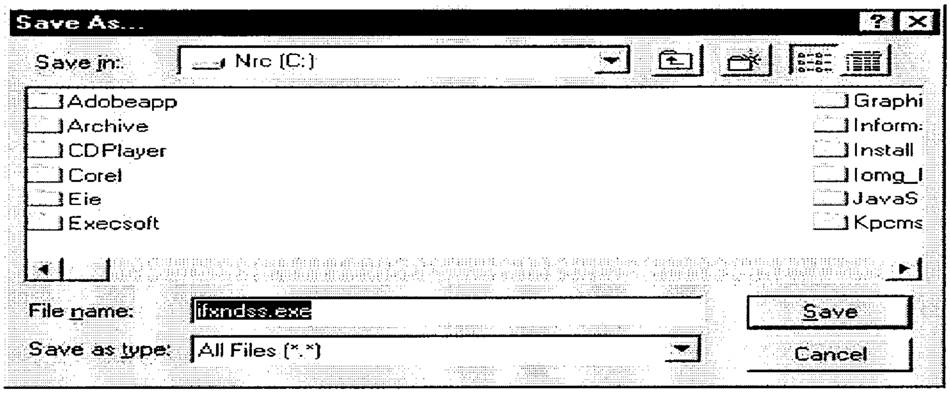
Step 2. Download and Install the Netscape Plug-in

(If you already have downloaded this and installed the Plug-in, go to step 3)

- Check to see if you already have the plug-in installed
- Download the Plug-in

Figure 2-27: Download the Plug-in

Step 2: The **Save As** window appears. Navigate to Drive C:\ and to a temporary folder in which you wish to save the file, IFXNDSS.EXE. The download will take approximately one minute on average. Click on **Save** and return to the EIE home page.

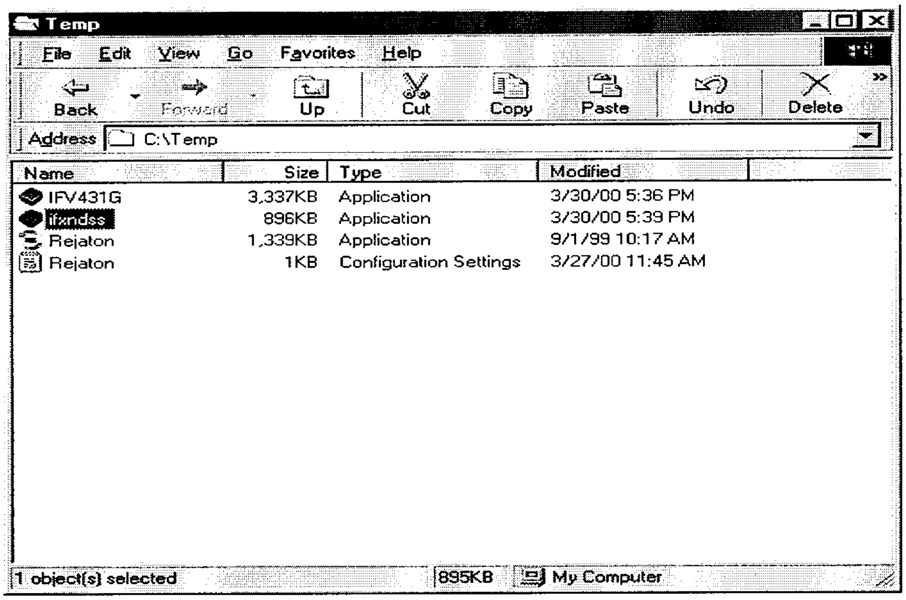


File name: ifxndss.exe

Save as type: All Files (*.*)

Figure 2-28: Save Netscape Signaturing File

Step 3: Close your Netscape browser and exit all other Windows applications before running the following setup programs. Access Drive C:\ and go to the temporary folder in which the plug-ins were saved. Install the InternetForms Extension for Netscape Digital Signature Support, IFXNDSS.EXE, by double-clicking the file icon. Follow the steps provided by the setup dialog.



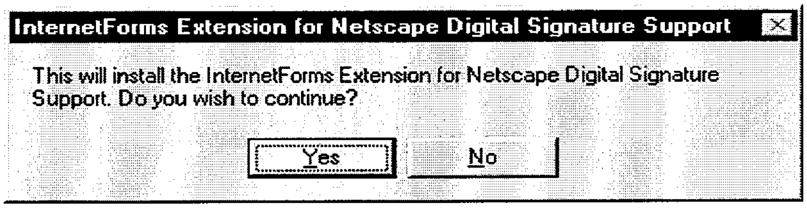
Address C:\Temp

Name	Size	Type	Modified
IFV431G	3,337KB	Application	3/30/00 5:36 PM
ifxndss	896KB	Application	3/30/00 5:39 PM
Rejaton	1,339KB	Application	9/1/99 10:17 AM
Rejaton	1KB	Configuration Settings	3/27/00 11:45 AM

1 object(s) selected 895KB My Computer

Figure 2-29: IFXNDSS.EXE File

Step 4: The install warning window appears.



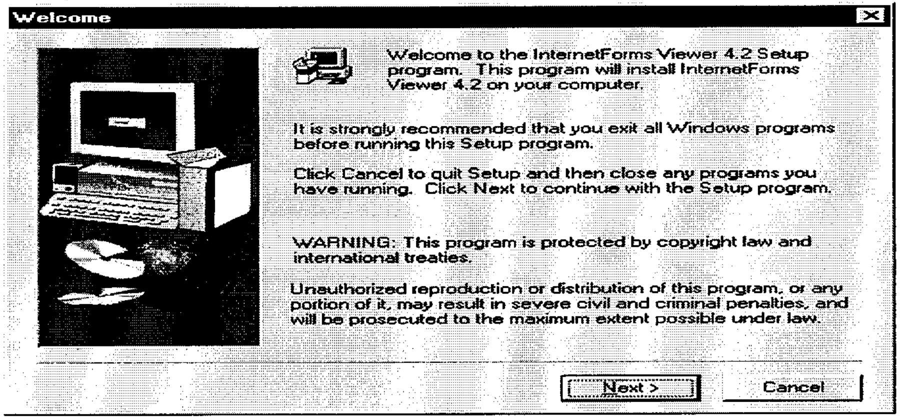
InternetForms Extension for Netscape Digital Signature Support

This will install the InternetForms Extension for Netscape Digital Signature Support. Do you wish to continue?

Figure 2-30: Install Warning Window

Click on the **Yes** button.

Step 5: The run setup window appears.



Welcome

Welcome to the InternetForms Viewer 4.2 Setup program. This program will install InternetForms Viewer 4.2 on your computer.

It is strongly recommended that you exit all Windows programs before running this Setup program.

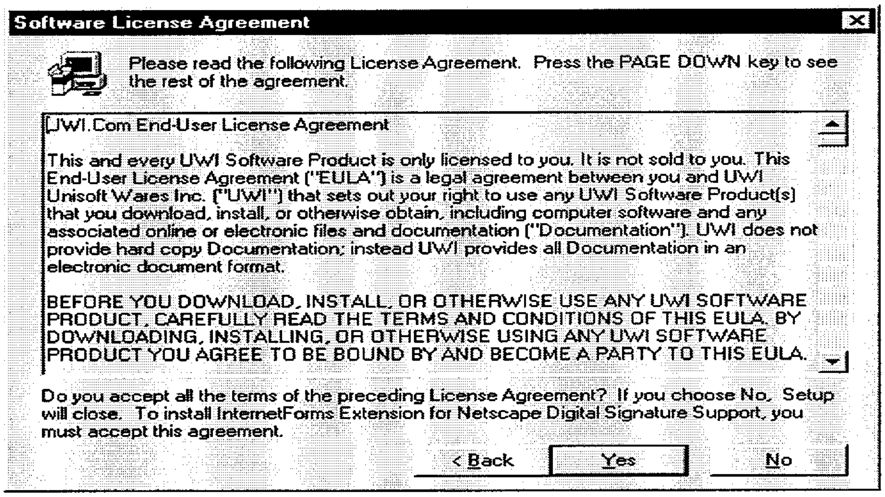
Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program.

WARNING: This program is protected by copyright law and international treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

Figure 2-31: Run setup window

Step 6: Run setup by clicking on the **Next** button. The Software License Agreement window appears.



Software License Agreement

Please read the following License Agreement. Press the PAGE DOWN key to see the rest of the agreement.

UWI.Com End-User License Agreement

This and every UWI Software Product is only licensed to you. It is not sold to you. This End-User License Agreement ("EULA") is a legal agreement between you and UWI Unisoft Wares Inc. ("UWI") that sets out your right to use any UWI Software Product(s) that you download, install, or otherwise obtain, including computer software and any associated online or electronic files and documentation ("Documentation"). UWI does not provide hard copy Documentation; instead UWI provides all Documentation in an electronic document format.

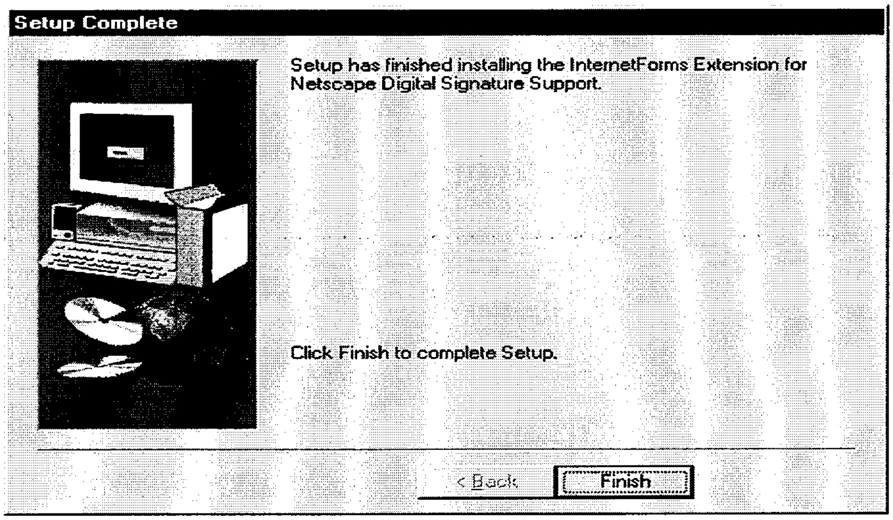
BEFORE YOU DOWNLOAD, INSTALL, OR OTHERWISE USE ANY UWI SOFTWARE PRODUCT, CAREFULLY READ THE TERMS AND CONDITIONS OF THIS EULA. BY DOWNLOADING, INSTALLING, OR OTHERWISE USING ANY UWI SOFTWARE PRODUCT YOU AGREE TO BE BOUND BY AND BECOME A PARTY TO THIS EULA.

Do you accept all the terms of the preceding License Agreement? If you choose No, Setup will close. To install InternetForms Extension for Netscape Digital Signature Support, you must accept this agreement.

Figure 2-32: Software License Agreement

Click on the **Yes** button to continue setup.

Step 7: When the setup is complete, the Setup Complete dialog box appears.



Setup Complete

Setup has finished installing the InternetForms Extension for Netscape Digital Signature Support.

Click Finish to complete Setup.

Figure 2-33: Setup Complete

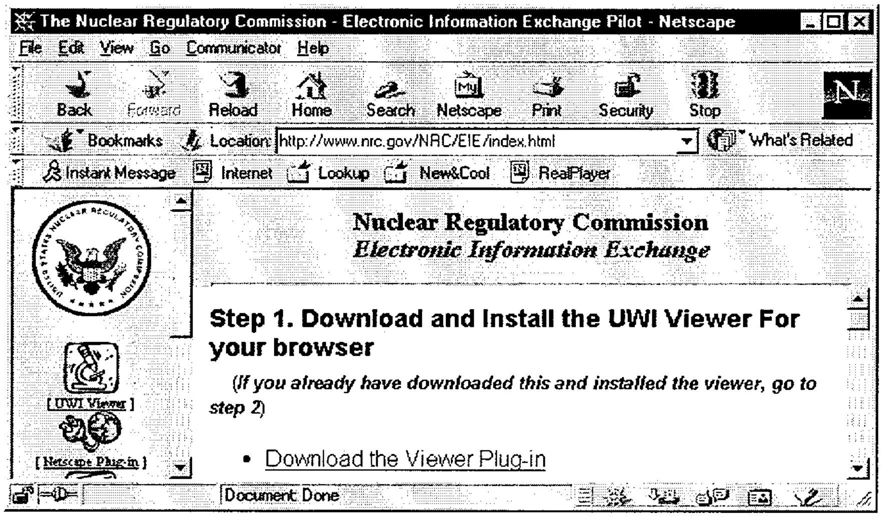
Click on the **Finish** button.

Participants using Netscape are now able to use their Digital ID for signaturing.

2.8 Obtaining the InternetForms Viewer

In order to properly utilize the form, participants will need the InternetForms Viewer. The viewer is a program that enables the form to be opened and read. The latest version of InternetForms, can be downloaded from the NRC EIE home page. The process for downloading the viewer is detailed below.

Step 1: Access the NRC EIE home page at http://www.nrc.gov/NRC/EIE/index.html. Upon connection, the NRC EIE home page appears.



The Nuclear Regulatory Commission - Electronic Information Exchange Pilot - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Location: http://www.nrc.gov/NRC/EIE/index.html What's Related
Instant Message Internet Lookup New&Cool RealPlayer
[UWI Viewer]
[Netscape Plug-in]
Document: Done

Nuclear Regulatory Commission
Electronic Information Exchange

Step 1. Download and Install the UWI Viewer For your browser

(If you already have downloaded this and installed the viewer, go to step 2)

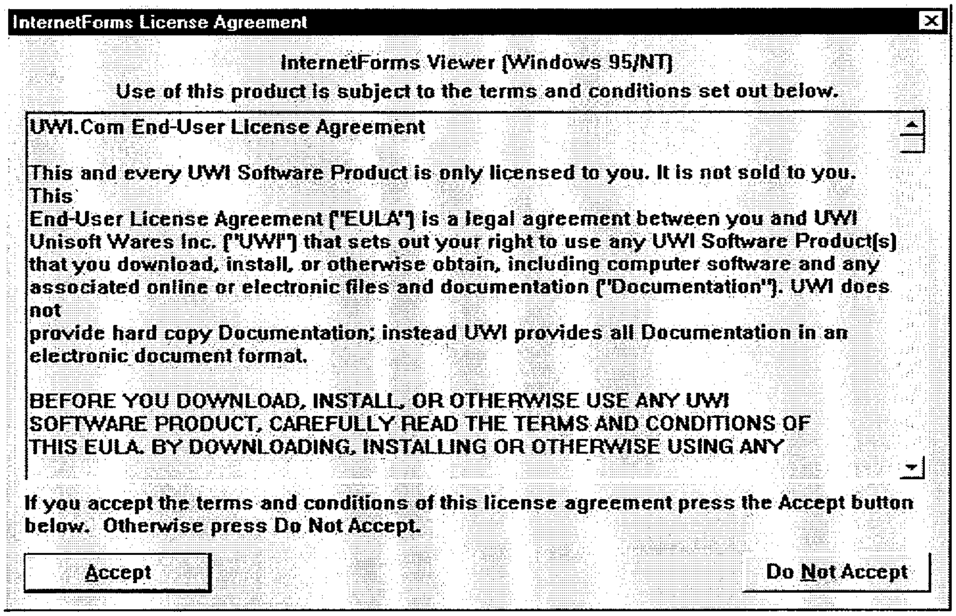
- Download the Viewer Plug-in

Figure 2-34: EIE Home Page

Step 2: Go to Step 1, "Download and Install the UWI Viewer for your browser." Click on **Download the Viewer Plug-in**. The download process varies depending on which browser you are using. The process for both Netscape and Microsoft Internet Explorer are outlined below.

Netscape Navigator/Communicator (version 4.6 or higher)

Step 3: Netscape users will receive the viewer license agreement as shown below.



InternetForms Viewer [Windows 95/NT]

Use of this product is subject to the terms and conditions set out below.

UWI.Com End-User License Agreement

This and every UWI Software Product is only licensed to you. It is not sold to you. This
End-User License Agreement ["EULA"] is a legal agreement between you and UWI Unisoft Wares Inc. ["UWI"] that sets out your right to use any UWI Software Product[s] that you download, install, or otherwise obtain, including computer software and any associated online or electronic files and documentation ["Documentation"]. UWI does not
provide hard copy Documentation; instead UWI provides all Documentation in an electronic document format.

BEFORE YOU DOWNLOAD, INSTALL, OR OTHERWISE USE ANY UWI SOFTWARE PRODUCT, CAREFULLY READ THE TERMS AND CONDITIONS OF THIS EULA. BY DOWNLOADING, INSTALLING OR OTHERWISE USING ANY

If you accept the terms and conditions of this license agreement press the Accept button below. Otherwise press Do Not Accept.

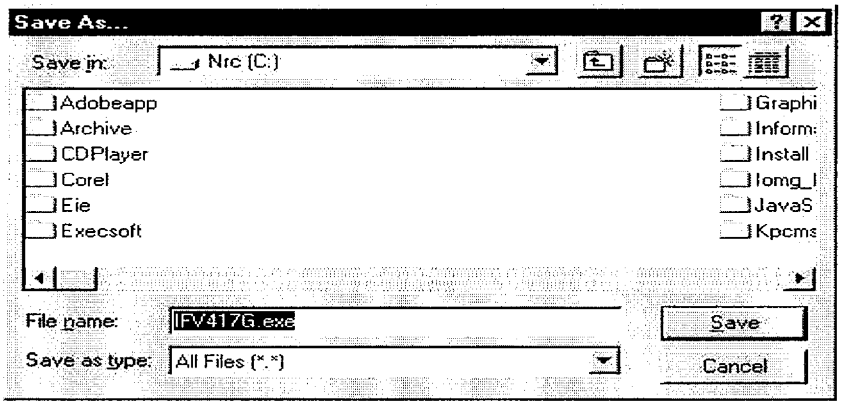
Figure 2-35: Viewer License Agreement

Read the viewer license agreement. If you accept the terms, click on **Accept** to begin the viewer download process.

Microsoft Internet Explorer (version 5.0 or higher)

Step 3a: Instead of the viewer license agreement, Internet Explorer users will receive the Save the file dialog as shown below.

Upon accepting the viewer license agreement or clicking on **Yes** to save the file, both Netscape and Internet Explorer users receive the save as dialog and the download and installation processes will proceed the same for each.



Save in: Nrc (C:)

File name: IFV417G.exe

Save as type: All Files (*.*)

Figure 2-36: Save Form Viewer File

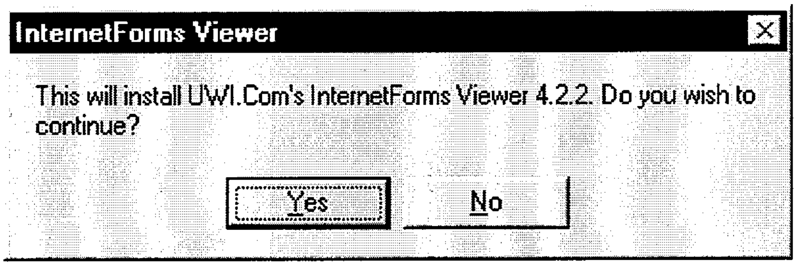
Step 4: From the Save As dialog, navigate to the appropriate drive and folder. (The default drive is C:\.) It is recommended that you save the file in a temporary (Temp) folder on your C:\ drive.

Step 5: Click on the **Save** button to save the downloaded file. Close the browser and install the viewer.

Installation:

Step 1: Navigate to the folder containing the downloaded file (file name, IFV431G.exe). Double click on the file icon.

Step 2: The InternetForms viewer warning appears.



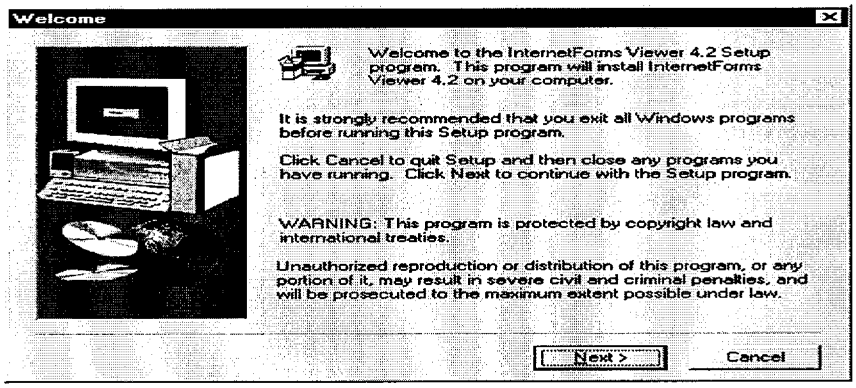
InternetForms Viewer

This will install UWI.Com's InternetForms Viewer 4.2.2. Do you wish to continue?

Figure 2-37: InternetForms Viewer Warning

Click on the **Yes** button to continue installation.

Step 3: The viewer setup begins and the Welcome window appears.



Welcome

Welcome to the InternetForms Viewer 4.2 Setup program. This program will install InternetForms Viewer 4.2 on your computer.

It is strongly recommended that you exit all Windows programs before running this Setup program.

Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program.

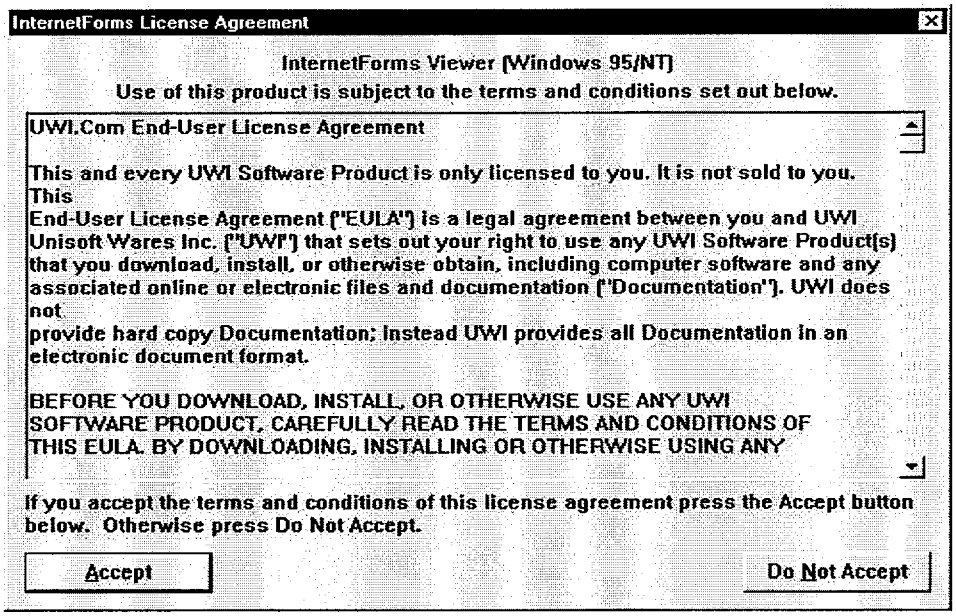
WARNING: This program is protected by copyright law and international treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

Figure 2-38: InternetForms Viewer Welcome Window

Click on **Next** to continue setup.

Step 4: The Software License Agreement dialog appears.



InternetForms Viewer (Windows 95/NT)
Use of this product is subject to the terms and conditions set out below.

UWI.Com End-User License Agreement

This and every UWI Software Product is only licensed to you. It is not sold to you.
This
End-User License Agreement ("EULA") is a legal agreement between you and UWI Unisoft Wares Inc. ("UWI") that sets out your right to use any UWI Software Product(s) that you download, install, or otherwise obtain, including computer software and any associated online or electronic files and documentation ("Documentation"). UWI does
not
provide hard copy Documentation; instead UWI provides all Documentation in an electronic document format.

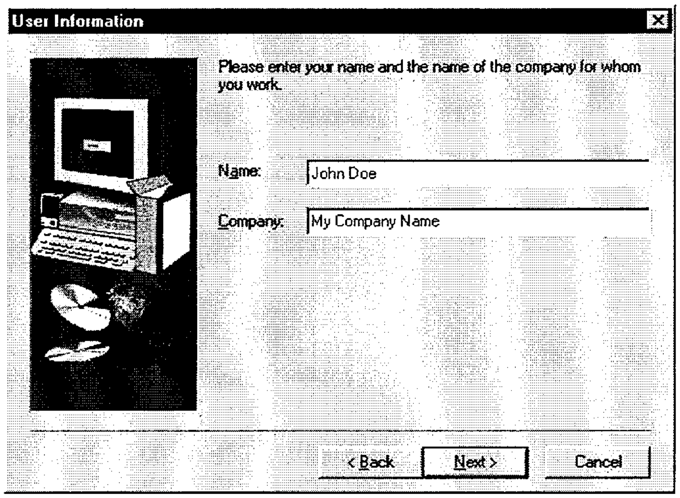
BEFORE YOU DOWNLOAD, INSTALL, OR OTHERWISE USE ANY UWI SOFTWARE PRODUCT, CAREFULLY READ THE TERMS AND CONDITIONS OF THIS EULA. BY DOWNLOADING, INSTALLING OR OTHERWISE USING ANY

If you accept the terms and conditions of this license agreement press the Accept button below. Otherwise press Do Not Accept.

Figure 2-39: Viewer License Agreement

Read the agreement. If you accept all the terms, click on **Yes** to accept it and continue setup.

Step 5: Next, the User Information window appears.



Please enter your name and the name of the company for whom you work.

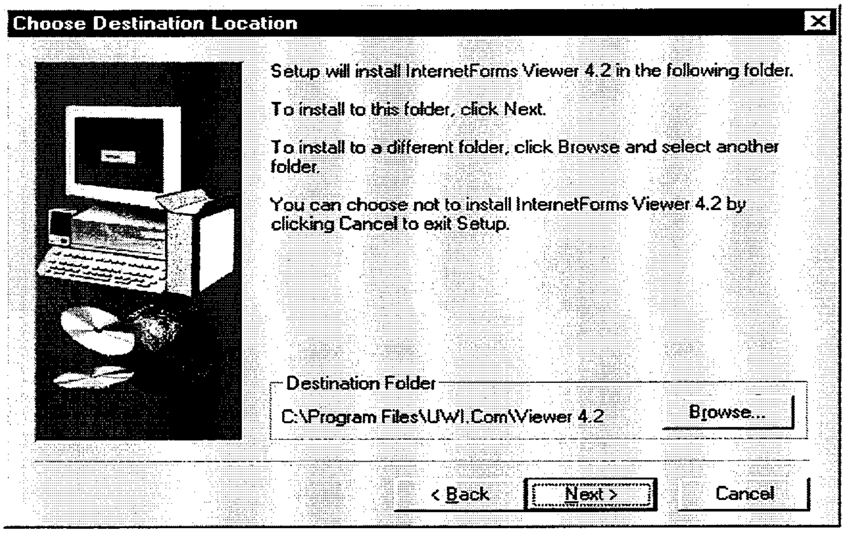
Name: John Doe

Company: My Company Name

Figure 2-40: User Information Window

Enter user information, participant name and company (agency) name. Click on **Next** to continue.

Step 6: Choose a destination location for the installation. (Note: Setup automatically creates a destination location (folder), however, you may click on **Browse** and select a different one.)



Setup will install InternetForms Viewer 4.2 in the following folder.

To install to this folder, click Next.

To install to a different folder, click Browse and select another folder.

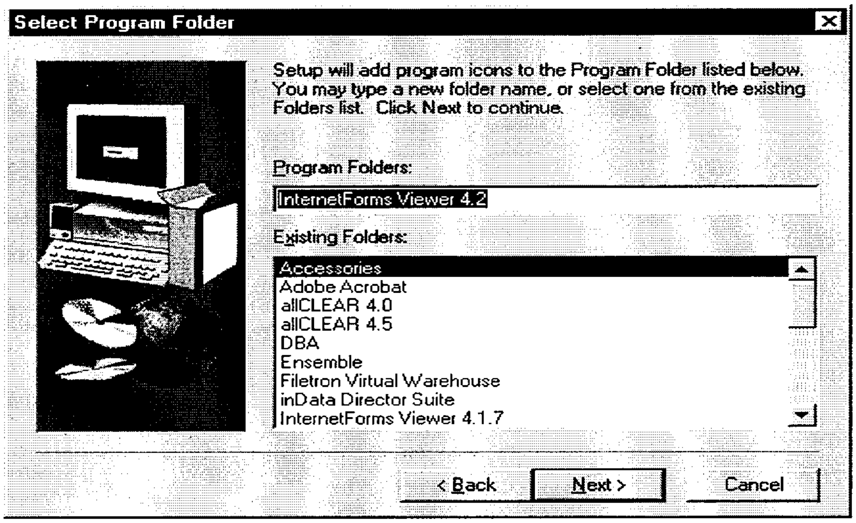
You can choose not to install InternetForms Viewer 4.2 by clicking Cancel to exit Setup.

Destination Folder: C:\Program Files\UWI.Com\Viewer 4.2

Figure 2-41: Choose Destination Location

Click on **Next** when done.

Step 7: Select a program folder. It is recommended that participants use the default folder, InternetForms Viewer 4.3.1.



Setup will add program icons to the Program Folder listed below. You may type a new folder name, or select one from the existing Folders list. Click Next to continue.

Program Folders: InternetForms Viewer 4.2

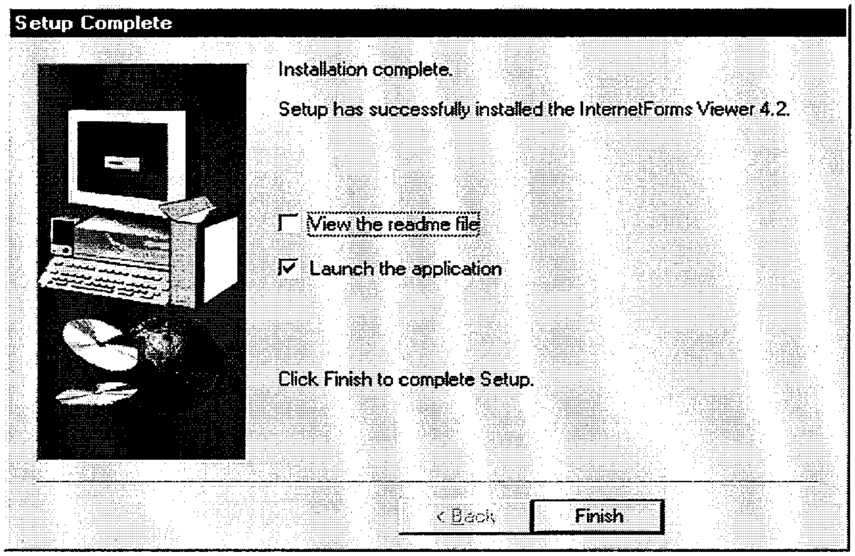
Existing Folders:

Accessories
Adobe Acrobat
allCLEAR 4.0
allCLEAR 4.5
DBA
Ensemble
Filetron Virtual Warehouse
inData Director Suite
InternetForms Viewer 4.1.7

Figure 2-42: Select Program Folder

Click on **Next** to continue.

Step 8: Setup runs and the setup complete window appears when done.



Setup Complete

Installation complete.

Setup has successfully installed the InternetForms Viewer 4.2.

☐ View the readme file

☑ Launch the application

Click Finish to complete Setup.

Figure 2-43: Setup Complete

Click on the **Finish** button to complete installation.

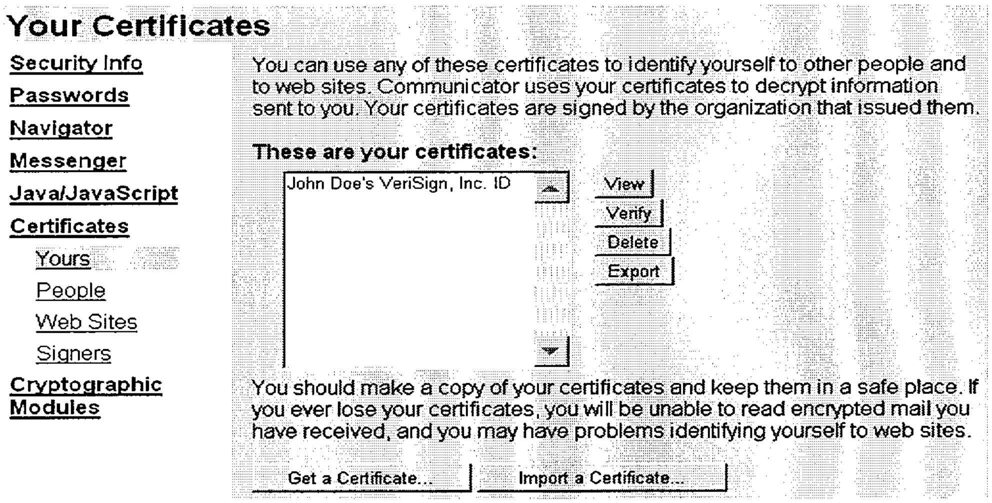
2.9 Providing Backup for Digital ID Certificates

EIE participants are responsible for the security of their own individual Digital ID certificates. In this regard, participants are encouraged to make a backup copy of their Digital ID. The steps applicable to each browser are outlined below.

Netscape Navigator/Communicator (version 4.6 or higher)

Netscape users can accomplish this in the following manner.

Step 1: Open the Security Advisor/Info window and select **Yours** from the left hand margin under Certificates. Highlight the Digital ID for backup and click on the **Export** button.



Your Certificates

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.

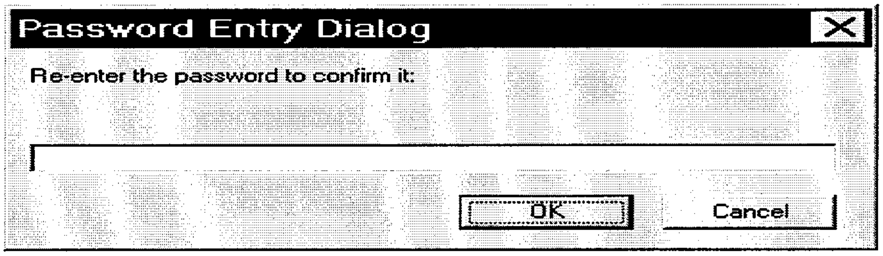
These are your certificates:

John Doe's VeriSign, Inc. ID

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.

Figure 2-44: Security Advisor/Window

Step 2: The Netscape Password Entry Dialog window appears. **Enter** your Netscape Certificate Database password. You will be prompted to specify another password to protect your Digital ID export file. **Confirm** the export file password a second time. Click on the **OK** button.

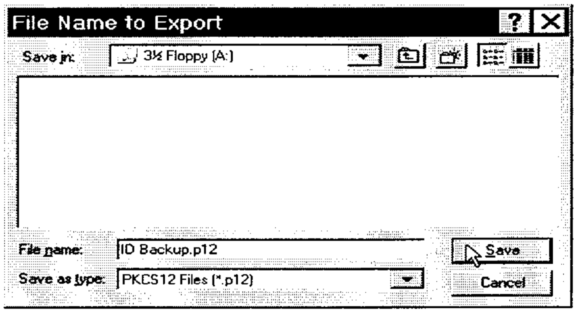


Password Entry Dialog

Re-enter the password to confirm it:

Figure 2-45: Password Entry Dialog

Step 3: The File Name to Export window appears. Name the file. The Digital ID is saved with a ".p12" file extension. It is recommended that you save your Digital ID on diskette and store the diskette in a safe and secure place. Click on the **Save** button.



File Name to Export

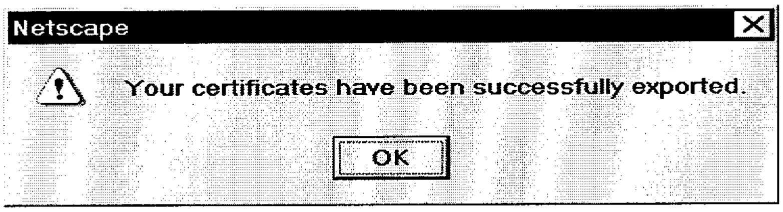
Save in: 3½ Floppy (A:)

File name: ID Backup.p12

Save as type: PKCS12 Files (*.p12)

Figure 2-46: File Name to Export Window

Step 4: A confirmation message appears when the Certificate has been successfully exported.



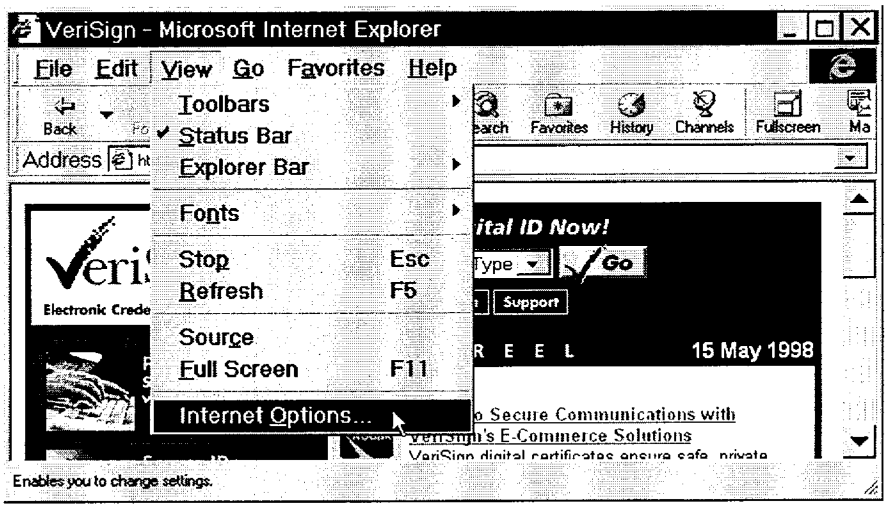
Netscape

Your certificates have been successfully exported.

Figure 2-47: Successful Export Message

Microsoft Internet Explorer (version 5.0 or higher)

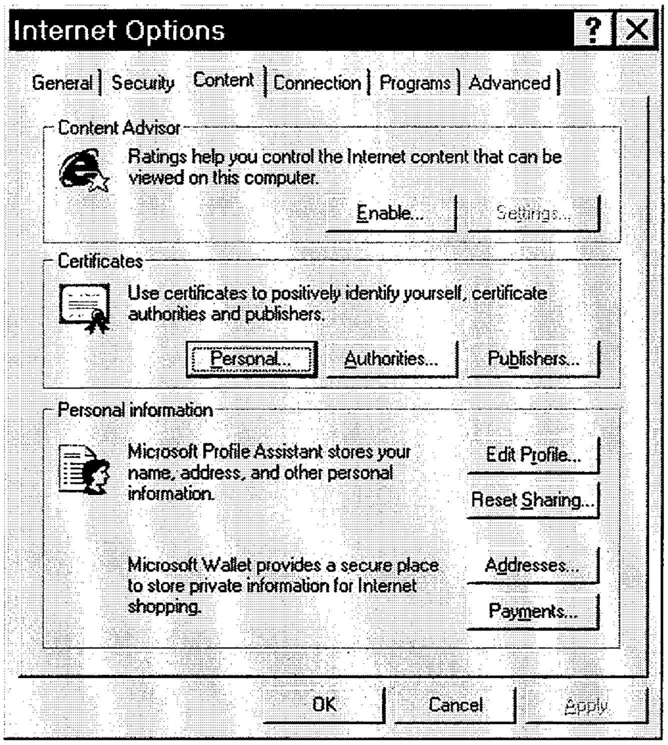
Step 1: Select **View** from the menu bar and click on **Internet Options** on the drop down menu.



VeriSign - Microsoft Internet Explorer
File Edit View Go Favorites Help
Back
Search Favorites History Channels Fullscreen Ma
Address
Toolbars
✓ Status Bar
Explorer Bar
Fonts
Stop Esc
Refresh F5
Source
Full Screen F11
Internet Options...
VeriSign
Electronic Crede
ital ID Now!
Type
Go
Support
R E E L
15 May 1998
o Secure Communications with
VeriSign's E-Commerce Solutions
VeriSign digital certificates ensure safe, private

Enables you to change settings.

Figure 2-48: Microsoft Menu Bar and Drop Down



Ratings help you control the Internet content that can be viewed on this computer.

Use certificates to positively identify yourself, certificate authorities and publishers.

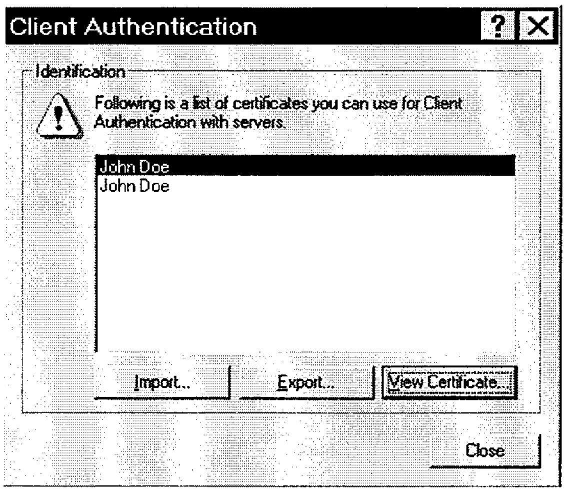
Microsoft Profile Assistant stores your name, address, and other personal information.

Microsoft Wallet provides a secure place to store private information for Internet shopping.

Figure 2-49: Internet Options Window

Step 2: In the Internet Options window, click on the tab labeled **Content**, click on the **Personal** button, and then click on the **OK** button.

The Client Authentication window appears.

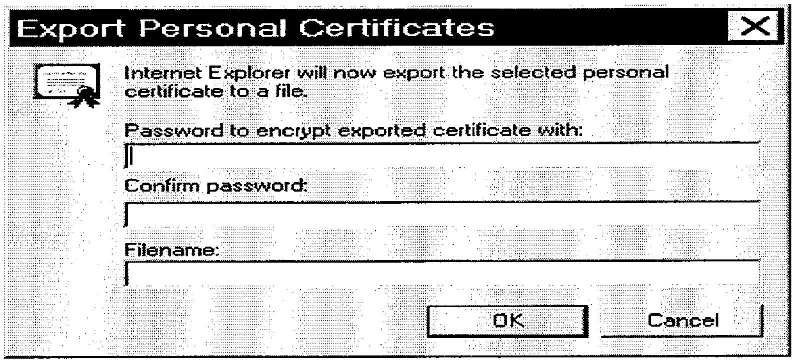


Following is a list of certificates you can use for Client Authentication with servers.

John Doe
John Doe

Figure 2-50: Client Authentication window

Step 3: Select and highlight the **Digital ID** to be exported. Click on the **Export** button. The Export Personal Certificates window appears.



Export Personal Certificates

Internet Explorer will now export the selected personal certificate to a file.

Password to encrypt exported certificate with:

Confirm password:

Filename:

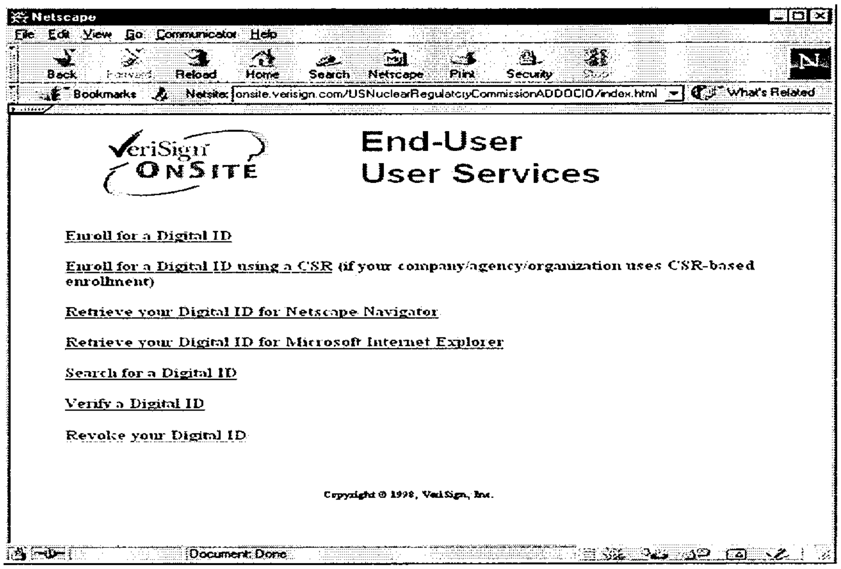
Figure 2-51: Export Personal Certificates Window

Step 4: In the Export Personal Certificates window, enter and confirm the password to be used to protect this file. Specify using a ".pfx" extension. Click on the **OK** button.

2.10 Replacing Digital ID Certificates

If the backup Digital ID certificate becomes misplaced, lost, or compromised, participants must revoke and replace their certificate and replace it. In the case of a lost, misplaced, or possibly compromised Digital ID certificate, participants should follow these steps to replace it.

Step 1: Access the enrollment page at the following URL: https://onsite.verisign.com/USNuclearRegulatoryCommissionADDOCIO/index.html



Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks
What's Related
VeriSign OnSite

Netsite: onsite.verisign.com/USNuclearRegulatoryCommissionADDOCIO/index.html

End-User
User Services

Enroll for a Digital ID

Enroll for a Digital ID using a CSR (if your company/agency/organization uses CSR-based enrollment)

Retrieve your Digital ID for Netscape Navigator

Retrieve your Digital ID for Microsoft Internet Explorer

Search for a Digital ID

Verify a Digital ID

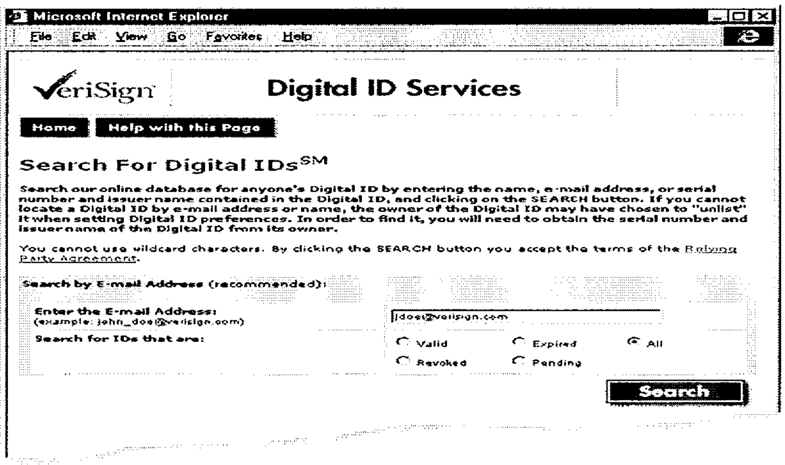
Revoke your Digital ID

Copyright © 1998, VeriSign, Inc.

Document: Done

Figure 2-52: NRC VeriSign Onsite Host Page

Step 2: Select the last option listed, **Revoke your Digital ID**. The Digital ID Search window appears.



Search For Digital IDs℠

Search our online database for anyone's Digital ID by entering the name, e-mail address, or serial number and issuer name contained in the Digital ID, and clicking on the SEARCH button. If you cannot locate a Digital ID by e-mail address or name, the owner of the Digital ID may have chosen to "unlist" it when setting Digital ID preferences. In order to find it, you will need to obtain the serial number and issuer name of the Digital ID from its owner.

You cannot use wildcard characters. By clicking the SEARCH button you accept the terms of the Relying Party Agreement.

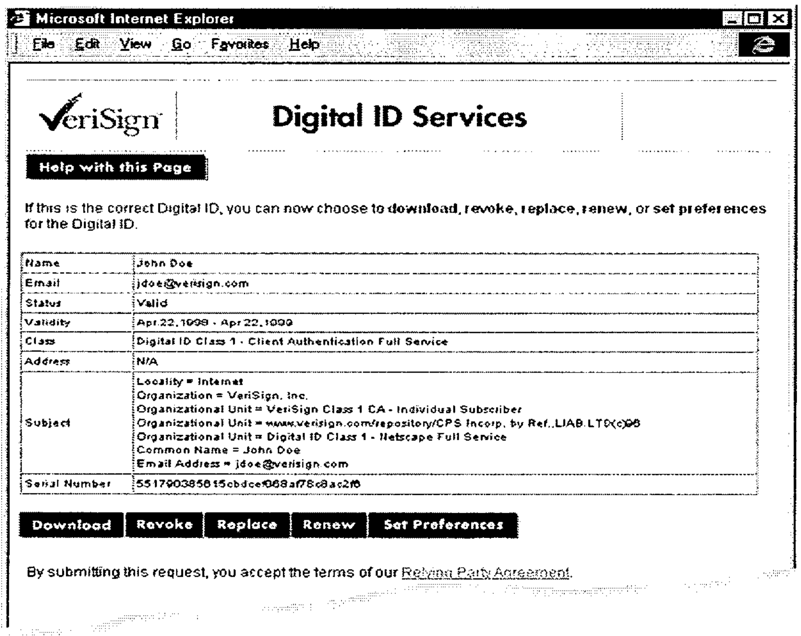
Search by E-mail Address (recommended):

Enter the E-mail Address: (example: john_doe@verisign.com) jdoe@verisign.com

Search for IDs that are: ○ Valid ○ Expired ● All ○ Revoked ○ Pending

Figure 2-53: Digital ID Search Window

Step 3: You will be prompted to search for the Digital ID. Enter you e-mail address to search for it. When the search is done, the result is displayed as follows.



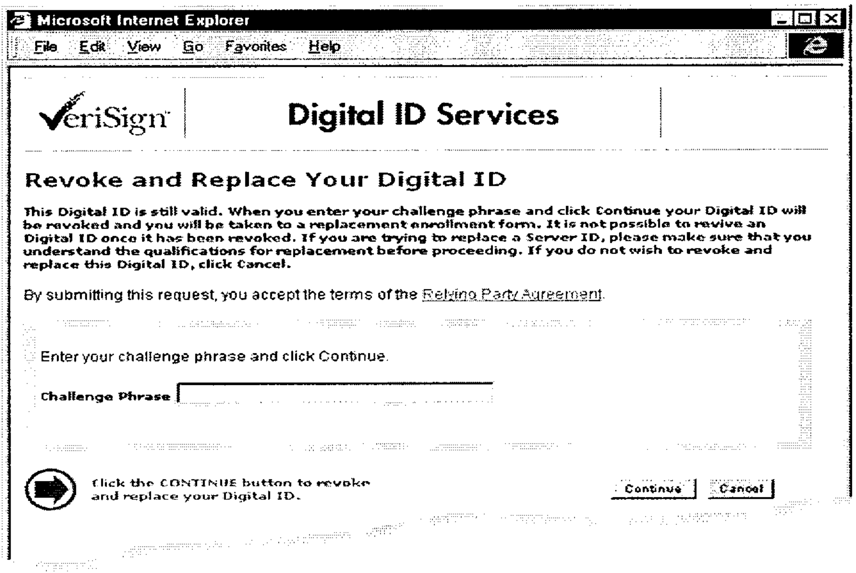
If this is the correct Digital ID, you can now choose to **download, revoke, replace, renew,** or **set preferences** for the Digital ID.

Name	John Doe
Email	jdoe@verisign.com
Status	Valid
Validity	Apr.22,1998 - Apr 22,1999
Class	Digital ID Class 1 - Client Authentication Full Service
Address	N/A
Subject	Locality = Internet Organization = VeriSign, Inc. Organizational Unit = VeriSign Class 1 CA - Individual Subscriber Organizational Unit = www.verisign.com/repository/CPS Incorp. by Ref.,LIAB.LTD(c)96 Organizational Unit = Digital ID Class 1 - Netscape Full Service Common Name = John Doe Email Address = jdoe@verisign.com
Serial Number	551790385815cbdcef068af78c8ac2f6

By submitting this request, you accept the terms of our Relying Party Agreement.

Figure 2-54: Digital ID Listed

Step 4: Click on the Replace button. The Revoke and Replace Your Digital ID window appears.



Revoke and Replace Your Digital ID

This Digital ID is still valid. When you enter your challenge phrase and click Continue your Digital ID will be revoked and you will be taken to a replacement enrollment form. It is not possible to revive an Digital ID once it has been revoked. If you are trying to replace a Server ID, please make sure that you understand the qualifications for replacement before proceeding. If you do not wish to revoke and replace this Digital ID, click Cancel.

By submitting this request, you accept the terms of the Relying Party Agreement.

Enter your challenge phrase and click Continue.

Challenge Phrase

Click the CONTINUE button to revoke and replace your Digital ID.

Figure: 2-55: Replace Digital ID Window

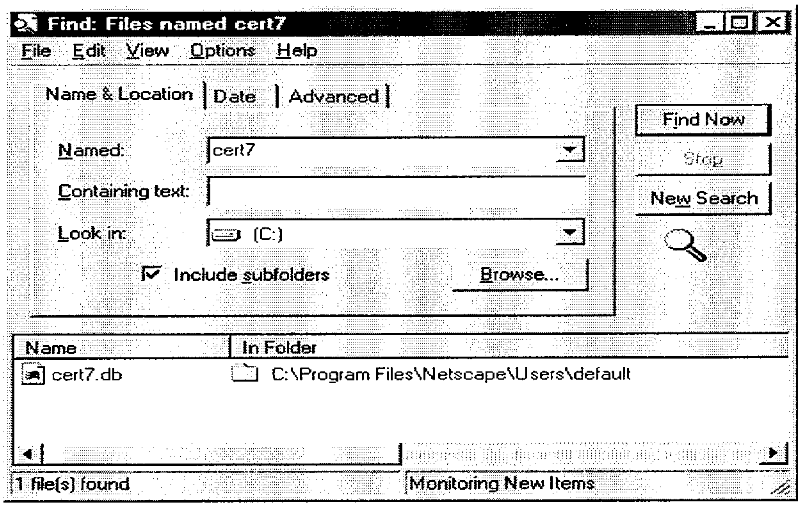
Step 5: Identify yourself by entering your "Challenge Phrase." Click on the **Continue** button to revoke your certificate and generate a new one.

Once the request for revocation and the issuance of a new Digital ID is complete, the new private key is generated and the request is forwarded tot he LRAA for action. From this point, the same processes outlined in sections 2.3 and 2.4 apply.

2.11 Replacing Netscape Digital ID Certificate Passwords

In the case of not being able to recall you password, Netscape users may replace their password as long as a copy of the Digital ID Certificate is on a diskette or the hard drive. If you do not have a copy of your Digital ID Certificate, you will not be able to replace your password, but rather follow the steps outlined above to replace the Digital ID. If you have a copy of your Digital Certificate, follow the steps below.

Step 1: Open Windows and locate the cert7.db file using Windows Explorer.


Find: Files named cert7

Named: cert7

Containing text:

Look in: (C:)

☑ Include subfolders

Name	In Folder
cert7.db	C:\Program Files\Netscape\Users\default

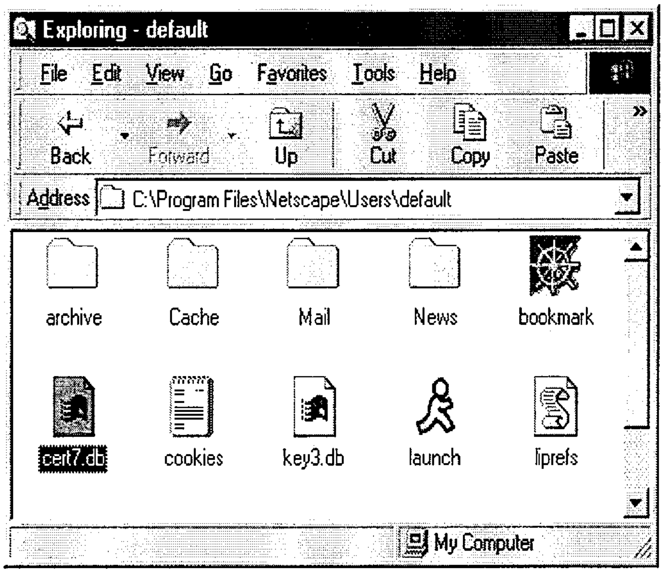
1 file(s) found

Monitoring New Items

Figure 2-56: Files named cert7.db in Windows explorer

For Windows 95/97/98 users, the file should be located in C:\Program Files\NETSCAPE\Users\your_name.

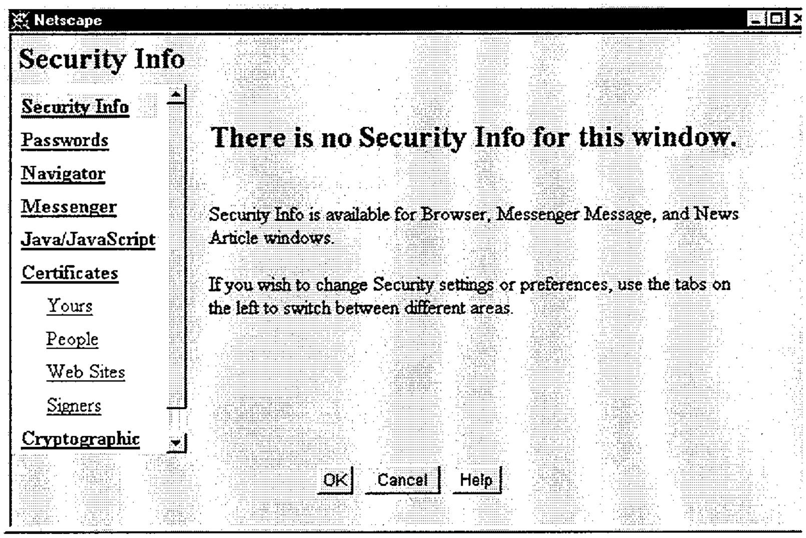
Step 2: Once located, delete the cert7.db file.


Exploring - default

Address C:\Program Files\Netscape\Users\default

Figure 2-57: Delete certificate window

Step 3: Open your browser and click on the Security icon to open the Security Advisor/Info window.



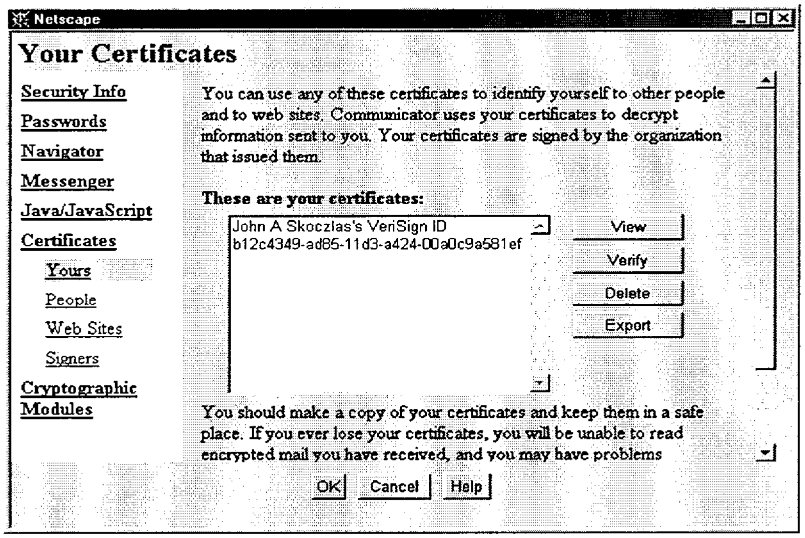
There is no Security Info for this window.

Security Info is available for Browser, Messenger Message, and News Article windows.

If you wish to change Security settings or preferences, use the tabs on the left to switch between different areas.

Figure 2-58: Security Advisor/Info Window

Step 4: In the Security Advisor/Info window, select **Yours** under Certificates.



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:

John A Skoczlas's VeriSign ID
b12c4349-ad85-11d3-a424-00a0c9a581ef

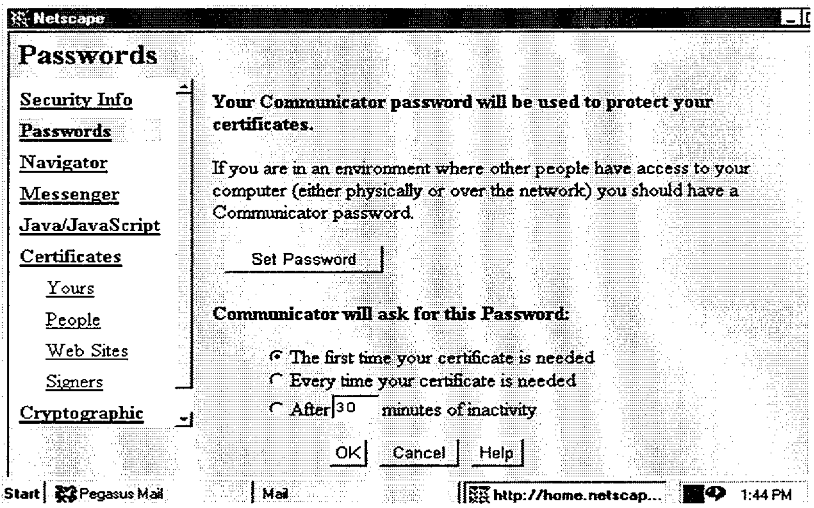
You should make a copy of your certificates and keep them in a safe place. If you ever lose your certificates, you will be unable to read encrypted mail you have received, and you may have problems

Figure 2-59: Your Certificates in Security Advisor/Info window

Step 5: From the certificates window, highlight your certificate and click on the **Delete** button. This will delete your certificate from your browser.

Step 6: Close your browser and restart Windows. Once windows has restarted, open your browser. Click on the **Security** icon to open the Security Advisor/Info window.

Step 7: In the Security Advisor/Info window, select **Passwords**. Click on the **Set Password** button to create a new password.



Your Communicator password will be used to protect your certificates.

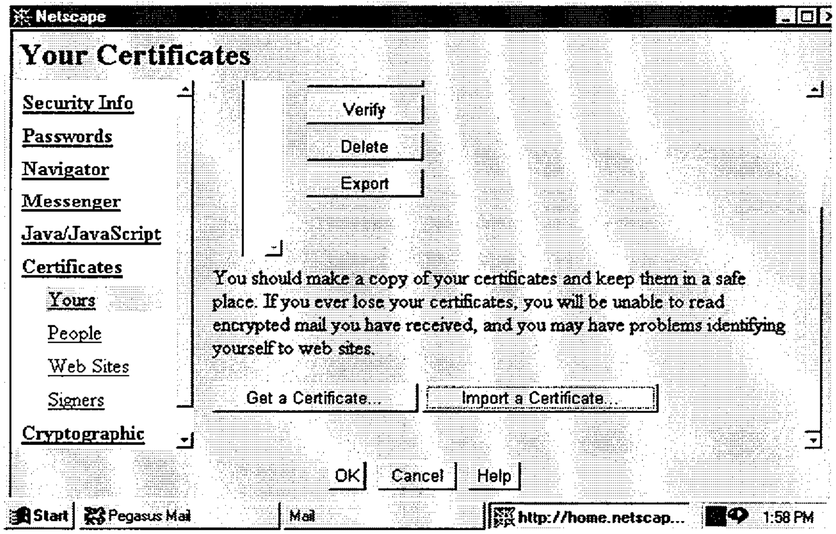
If you are in an environment where other people have access to your computer (either physically or over the network) you should have a Communicator password.

Communicator will ask for this Password:

● The first time your certificate is needed
○ Every time your certificate is needed
○ After 30 minutes of inactivity

Figure: 2-60: Set Password

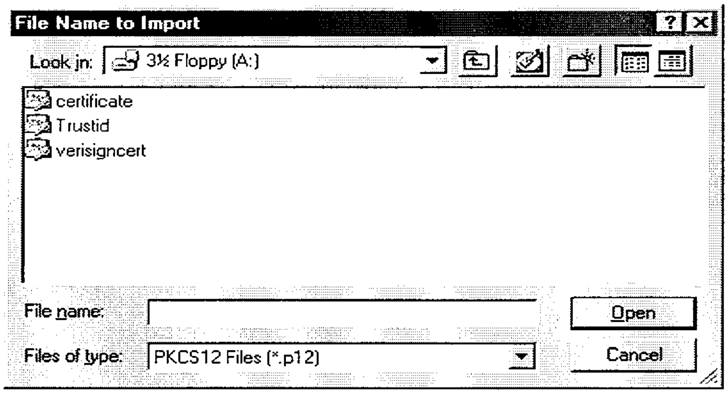
Step 8: After creating a new password, select <u>**Yours**</u> under certificates. Use the right-hand scroll bar to scroll to the bottom of the certificates window. Click on **Import a Certificate**. Insert the diskette containing your certificate in drive A: or wait for the prompt to navigate to drive C: (if your certificate is saved there).



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.

Figure 2-61: Import a Certificate

Step 9: This invokes the Password Entry Dialog. Enter the new password and click on **<u>O</u>K**. This opens the File Name to Import window.



File Name to Import

Look in: 3½ Floppy (A:)

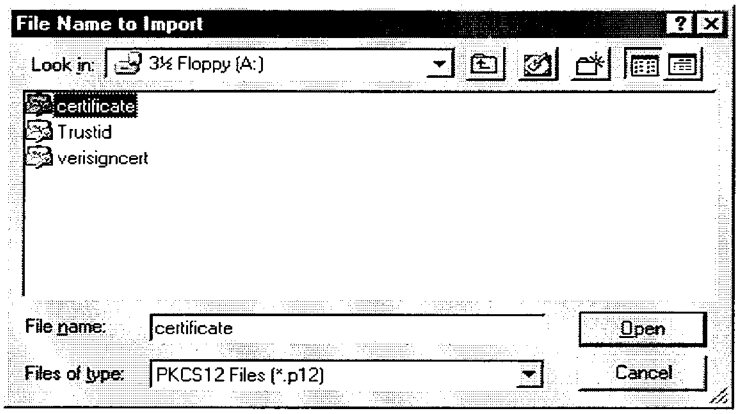
certificate
Trustid
verisigncert

File name:

Files of type: PKCS12 Files (*.p12)

Figure 2-62: File Name to Import Window

Step 10: Insert the diskette containing your certificate in drive A: or wait for the prompt to navigate to drive C: (if your certificate is saved there). Locate the certificate begin the import process by either double clicking on the certificate icon or by highlighting it and clicking the **Open** button.



File Name to Import

Look in: 3½ Floppy (A:)

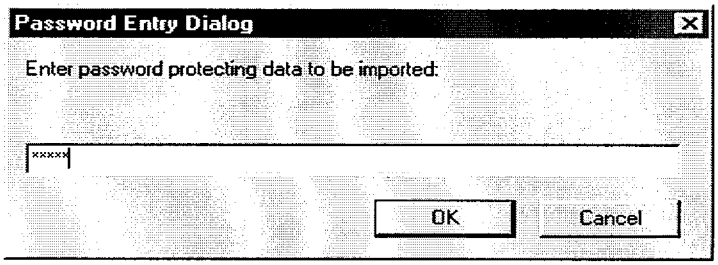
certificate
Trustid
verisigncert

File name: certificate

Files of type: PKCS12 Files (*.p12)

Figure 2-63: File Name to Import Window

Step 11: The Password Entry Dialog now opens. Enter the password for the file to be imported. (This is the password assigned when the certificate was first backed-up. See Section 2.8). Click on the **OK** button.



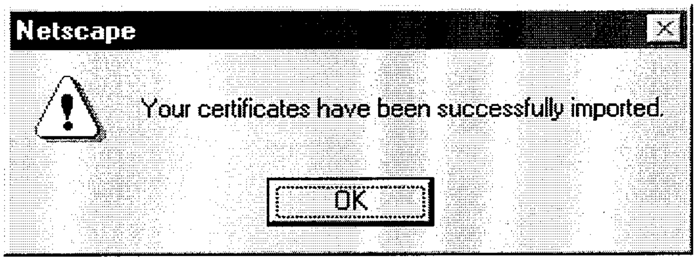
Password Entry Dialog

Enter password protecting data to be imported:

*****

Figure 2-64: Password Entry Dialog

Step 12: Netscape then displays a message stating that the certificate has been successfully imported.



Your certificates have been successfully imported.

Figure 2-65: Successfully Imported Certificate

Click on the **OK** button. Return to the Security Advisor/Info window and exit the browser. Once the certificate has been successfully imported, you may use it again in conjunction with your new password.

3.0 HOW TO SUBMIT DOCUMENTS

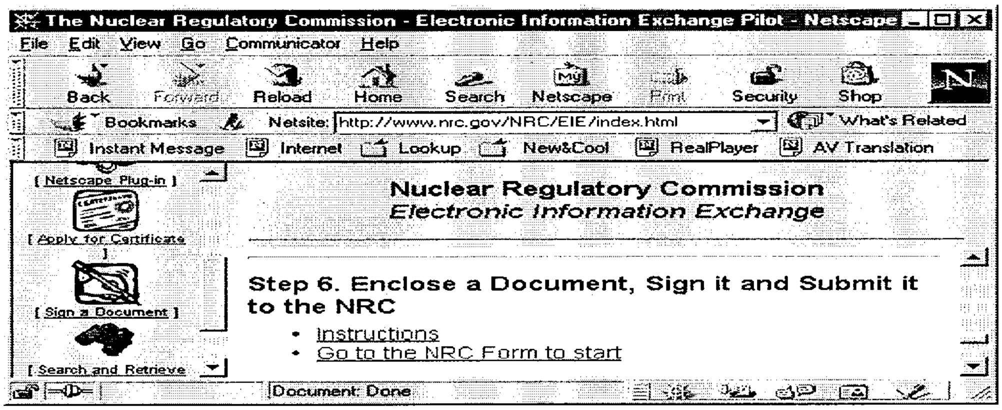
3.1 Introduction

Documents eligible for submission to the NRC or for transmission from the NRC are restricted to specific formats. It is expected that documents will be submitted in one of the following formats: MS Word, WordPerfect, PDF Image with Embedded Text, PDF Normal, Multi-page TIFF, ASCII Text, MS PowerPoint, Quattro Pro, or MS Excel. Participants shall use the NRC EIE Form (form) to submit or transmit documents. The form shall contain, as an enclosure, the document(s) to be submitted or transmitted. In addition, each form submitted must be digitally signed. In order to open and read a form, each participant shall require a form viewer. The steps necessary to perform each of these processes are described in the following sections.

3.2 How to Obtain the NRC EIE Form

The submission or transmission of EIE documents will require the use of the NRC EIE form. The EIE form is an intelligent document based on Extensible Machine Language (XML). It allows participants to sign, enclose, submit, and verify documents via the Internet. Participants may choose to simply access the form via the NRC EIE home page each time they wish to submit a document. Similar to the viewer, the form can be obtained by following the steps outlined below.

Step 1: Access the NRC EIE home page at http://www.nrc.gov/EIE/index.html. Once connected, go to Step 6 and click on **Go to the NRC Form**.


The Nuclear Regulatory Commission - Electronic Information Exchange Pilot - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop
Bookmarks Netsite: http://www.nrc.gov/NRC/EIE/index.html What's Related
Instant Message Internet Lookup New&Cool RealPlayer AV Translation
[Netscape Plug-in]
[Apply for Certificate]
[Sign a Document]
[Search and Retrieve
Document: Done

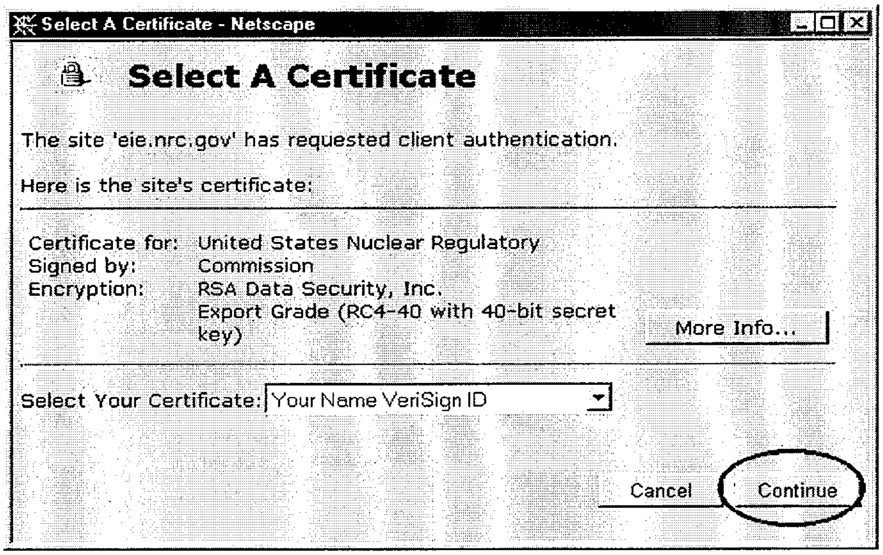
Nuclear Regulatory Commission
Electronic Information Exchange

Step 6. Enclose a Document, Sign it and Submit it to the NRC

- Instructions
- Go to the NRC Form to start

Figure 3-1: NRC EIE Home Page

Step 2: The "Select a Certificate" window appears. (Note: In order to access the EIE server and retrieve documents, each participant must have an NRC issued Digital ID certificate).



The site 'eie.nrc.gov' has requested client authentication.

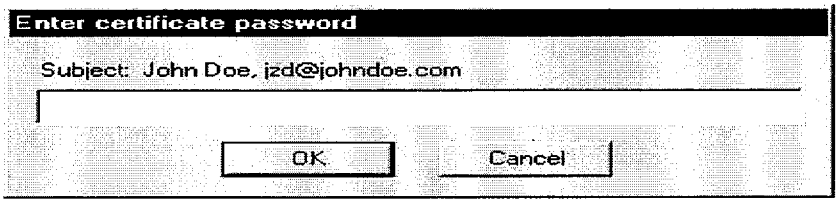
Here is the site's certificate:

Certificate for: United States Nuclear Regulatory
Signed by: Commission
Encryption: RSA Data Security, Inc.
Export Grade (RC4-40 with 40-bit secret key)

Select Your Certificate: Your Name VeriSign ID

Figure 3-2: Select a certificate

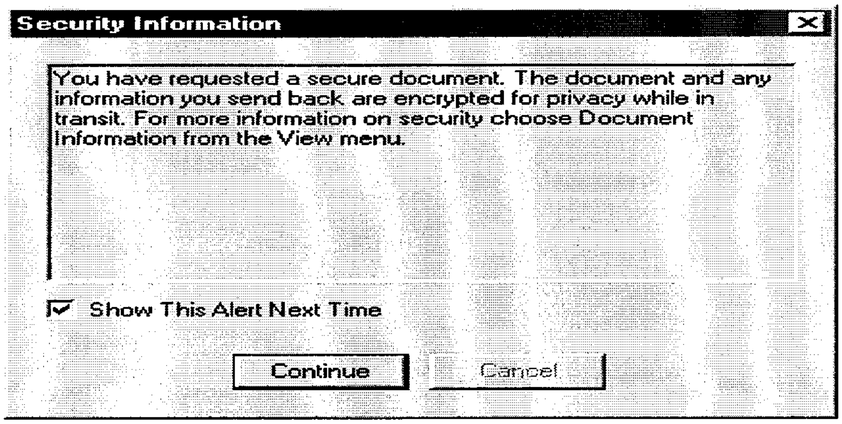
Select your NRC issued certificate and click on the **Continue** button. The Password Entry dialog appears.



Subject: John Doe, jzd@johndoe.com

Figure 3-3: Netscape Password Dialog Box

Step 3: Enter your password for the Certificate Database and click on **OK**. You will be prompted to re-enter it for confirmation, click on the **OK** button. A Security Information window appears, click on **Continue**.

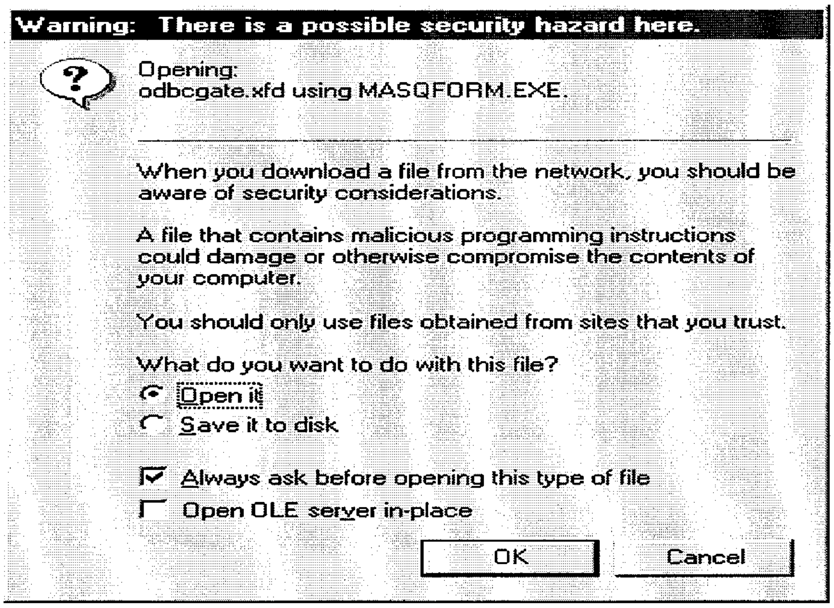


You have requested a secure document. The document and any information you send back are encrypted for privacy while in transit. For more information on security choose Document Information from the View menu.

☑ Show This Alert Next Time

Figure 3-4: Security Information Window

Step 4: The Security Warning window appears. Click on **OK** to continue.



Warning: There is a possible security hazard here.

Opening:
odbcgate.xfd using MASQFORM.EXE.

When you download a file from the network, you should be aware of security considerations.

A file that contains malicious programming instructions could damage or otherwise compromise the contents of your computer.

You should only use files obtained from sites that you trust.

What do you want to do with this file?

● Open it

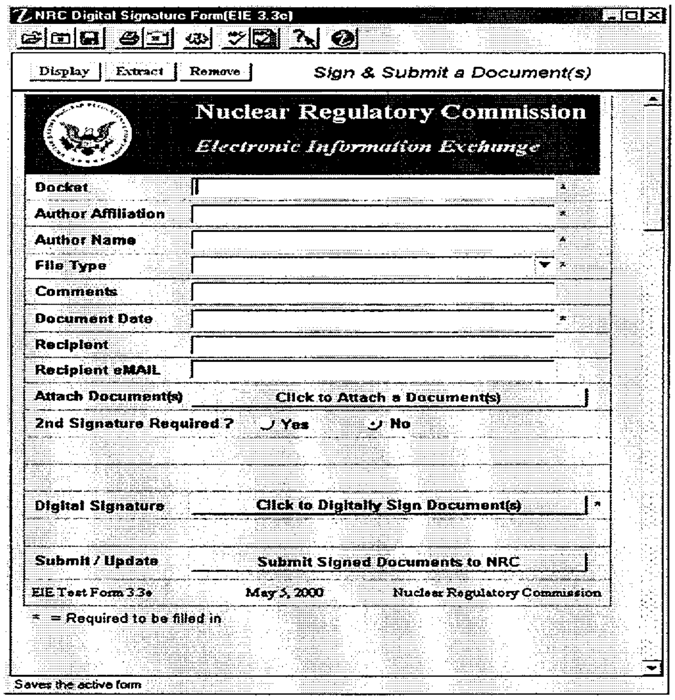
○ Save it to disk

☑ Always ask before opening this type of file

□ Open OLE server in-place

Figure 3-5: Security Warning Window

The PureEdge InternetForms viewer is loaded and the NRC EIE Form is displayed.



NRC Digital Signature Form(EIE 3.3c)

Sign & Submit a Document(s)

Nuclear Regulatory Commission

Electronic Information Exchange

Docket	*
Author Affiliation	*
Author Name	*
File Type	*
Comments	
Document Date	*
Recipient	
Recipient eMAIL	
Attach Document(s)	Click to Attach a Document(s)
2nd Signature Required ?	○ Yes ● No
Digital Signature	Click to Digitally Sign Document(s) *
Submit / Update	Submit Signed Documents to NRC

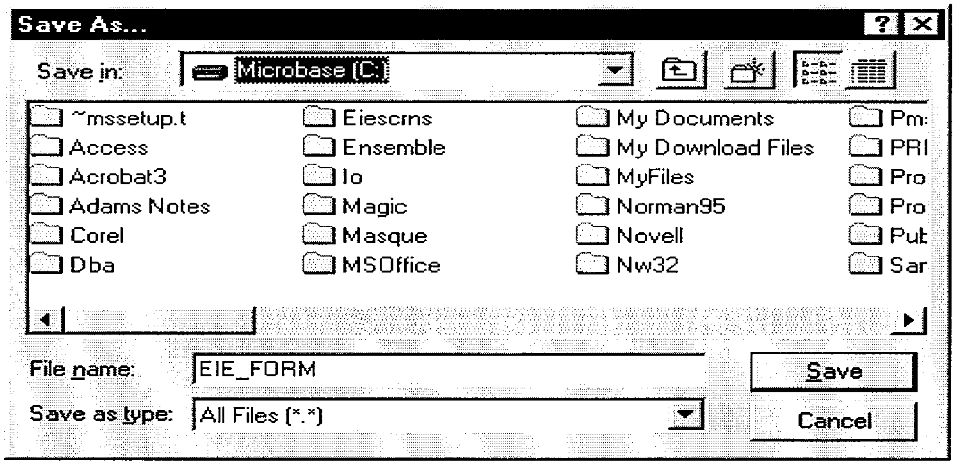
EIE Test Form 3.3e May 5, 2000 Nuclear Regulatory Commission

* = Required to be filled in

Saves the active form

Figure 3-6: NRC EIE Form

Step 5: If you wish to download the form, select **File** from the browser's menu bar and click on **Save As**. This invokes the Save As dialog box.



Save in: Microbase (C:)

File name: EIE_FORM

Save as type: All Files (*.*)

Figure 3-7: Save as Dialog Box

Step 6: Select the drive and directory in which you wish to save the form and click on the **Save** button. (The default drive is the C:\ drive.)

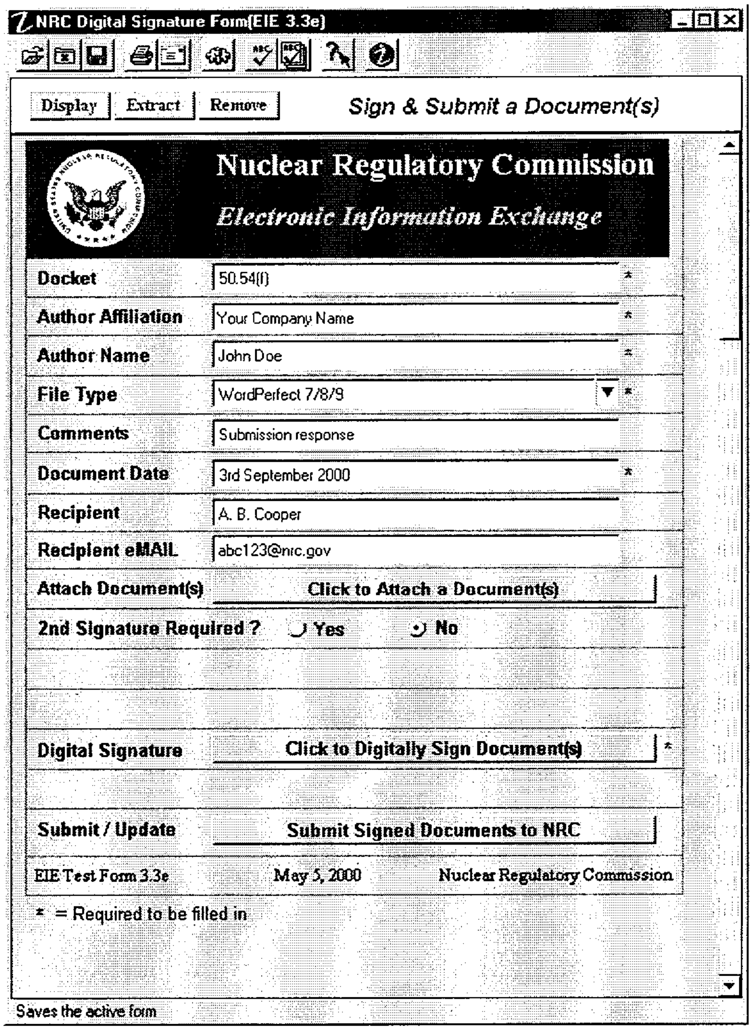
3.3 How to Complete the Form

The NRC EIE form contains several fields for bibliographic information. The form's bibliographic fields are listed and described in Table 3-1 below.

Field Name	Description	Required Y/N
Docket Number	The document's NRC docket number(s), i.e., 50-424 and/or 50-425.	Y
Author Affiliation	The agency, department, or company name of the document's author.	Y
Author Name	The author(s) of the document(s).	Y
File Type	The document's file type, i.e., "Adobe PDF," or Corel WordPerfect 6/7/8.	Y
Document Date	The date of the Form Submittal.	Y
Comments	General notes pertaining to the document(s).	N
Recipient	Name(s) of those to whom the document(s) is addressed.	Y
Recipient E-Mail	E-mail address(es) of those to whom the document(s) is addressed.	Y

Table 3-1: NRC EIE Form Bibliographic Fields

Information must be entered into all fields with the exception of the "Comments" field which is optional. The required fields are denoted on the form by a red (*). Participants should take care to ensure that these fields are complete before attempting to submit the form. If an attempt is made to submit where any of these fields are left blank, the form's submit function will not activate and the field(s) with missing information will be highlighted. This process interruption will occur until the empty fields are filled. Upon completion of the bibliographic information, the form should look similar to the one below.


NRC Digital Signature Form(EIE 3.3e)
Display
Extract
Remove
Sign & Submit a Document(s)
Nuclear Regulatory Commission
Electronic Information Exchange

Docket	50.54(f)	*
Author Affiliation	Your Company Name	*
Author Name	John Doe	*
File Type	WordPerfect 7/8/9	*
Comments	Submission response	
Document Date	3rd September 2000	*
Recipient	A. B. Cooper	
Recipient eMAIL	abc123@nrc.gov	
Attach Document(s)	Click to Attach a Document(s)	
2nd Signature Required ?	○ Yes ● No	
Digital Signature	Click to Digitally Sign Document(s)	*
Submit / Update	Submit Signed Documents to NRC	

EIE Test Form 3.3e May 5, 2000 Nuclear Regulatory Commission

* = Required to be filled in

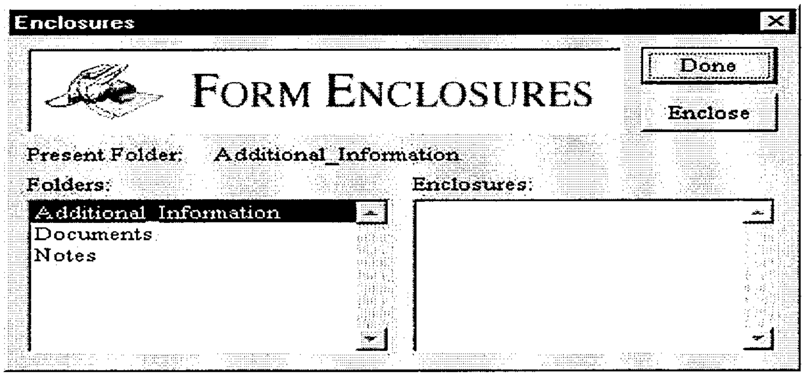
Saves the active form

Figure 3-8: Completed NRC EIE Form

3.4 How to Enclose Documents

Once the viewer has been downloaded and installed, participants can utilize the form to collect documents for submission or transmission. This process is called enclosing or attaching documents. Each submittal shall be comprised of two parts, the EIE form and the documentary material(s) for submission. The contents of a form package consists of the collection of documentary material(s). Participants can enclose or attach documents by following the steps below.

Step 1: With the form open, click on the **Click to Attach a Document(s)** button. The Enclosures Dialog box appears.

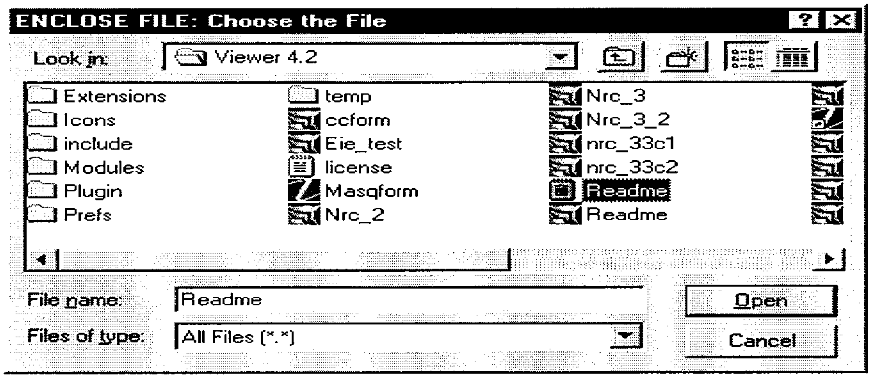


Present Folder: Additional_Information

Figure 3-9: Enclosures Dialog Box

The Enclosures dialog box displays three folders on the left side. The "Documents" folder is used for documents, the "Additional Information" folder is used for supporting information, and the "Notes" folder is used for comments or notes. Select the "Documents" folder to enclose your document(s) by highlighting it.

Step 2: Click on the Enclose button in the upper right corner of the dialog box. This opens the Enclose File window that allows you to browse your drives and find the document(s) you wish to enclose.



Look in: Viewer 4.2

File name: Readme

Files of type: All Files (*.*)

Figure 3-10: Enclose File Window

Step 3: Within the window, navigate to the document to be enclosed. Select the document or file and enclose it by double clicking on it or by clicking to highlight it and then clicking on the **Open** button.

Step 4: After selecting the document or file, the Enclosures dialog box re-appears. The name of the chosen document or file appears in the enclosures directory on the right side of the dialog box with it's native application extension as shown below.

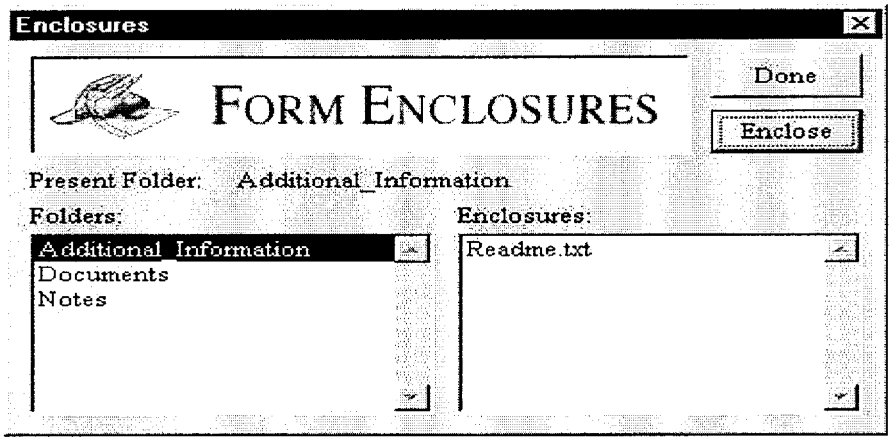


Figure 3-11: Form Enclosure Window

Step 5: To add additional documents or files for enclosure, repeat steps 2 and 3. When all necessary documents or files have been enclosed, click on the **Done** button.

There is no limit to the number of documents that can be enclosed. However, the file size for submittals is restricted to no more than 15 MB including the form which is approximately 40-50 KB.

After enclosing the document(s) necessary for submission, the form and its contents are ready for signing.

3.5 How to Sign (or Unsign) Forms

All documents submitted or transmitted shall be signed using digital signature software. It is recognized that the submitter of a document may not be its author. As such, the objective is to validate the identity of the submitter and to authenticate the document(s) submitted. The form contains a signature field designed to allow participants to digitally sign it. Once the bibliographic information has been completed and the necessary documents enclosed, participants can sign the form by following the steps outlined below.

Step 1: With the completed form open, click on the **Click to Digitally Sign Document(s)** button. Upon doing so, the Digital Signature Viewer dialog box appears.

The Digital Signature Viewer displays the caption "No Signature." This indicates that the form has not been signed. If you have a Digital ID Certificate, the **Sign** button is highlighted.

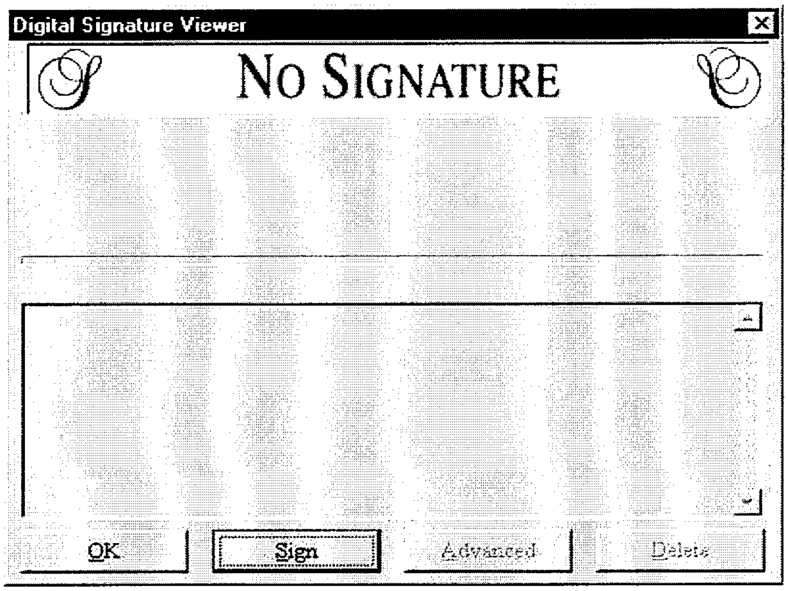
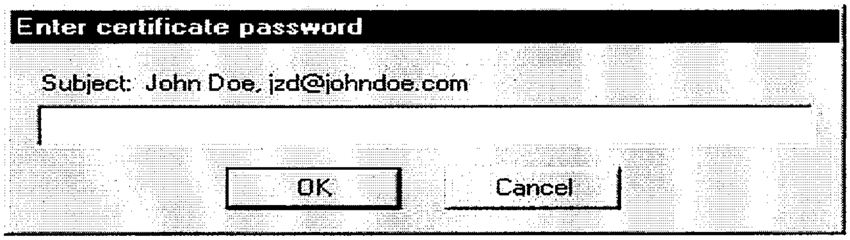


Figure 3-12: Digital Signature Viewer Dialog Box

Step 2: Click on the **Sign** button. The form will attempt to look up your Digital ID Certificate.

Step 3: At this point, Netscape users are asked for the password to their Certificate Database.

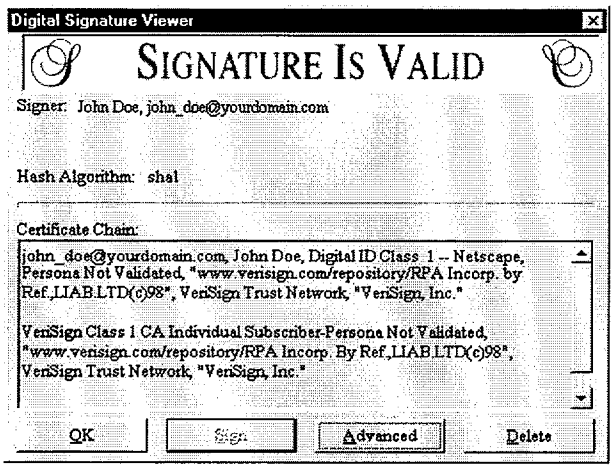


Subject: John Doe, jzd@johndoe.com

Figure 3-13: Netscape Password Window

Enter password and click on the **OK** button.

This initiates the signaturing process that retrieves the Digital ID Certificate stored in the browser. If successful, the viewer displays information pertaining to the signer such as the signer's name and e-mail address, the signature's hash algorithm, the certificate chain stating the name of the certificate authority that provided the signature certificate, and the class of certificate as illustrated below.



Digital Signature Viewer

SIGNATURE IS VALID

Signer: John Doe, john_doe@yourdomain.com

Hash Algorithm: shal

Certificate Chain:

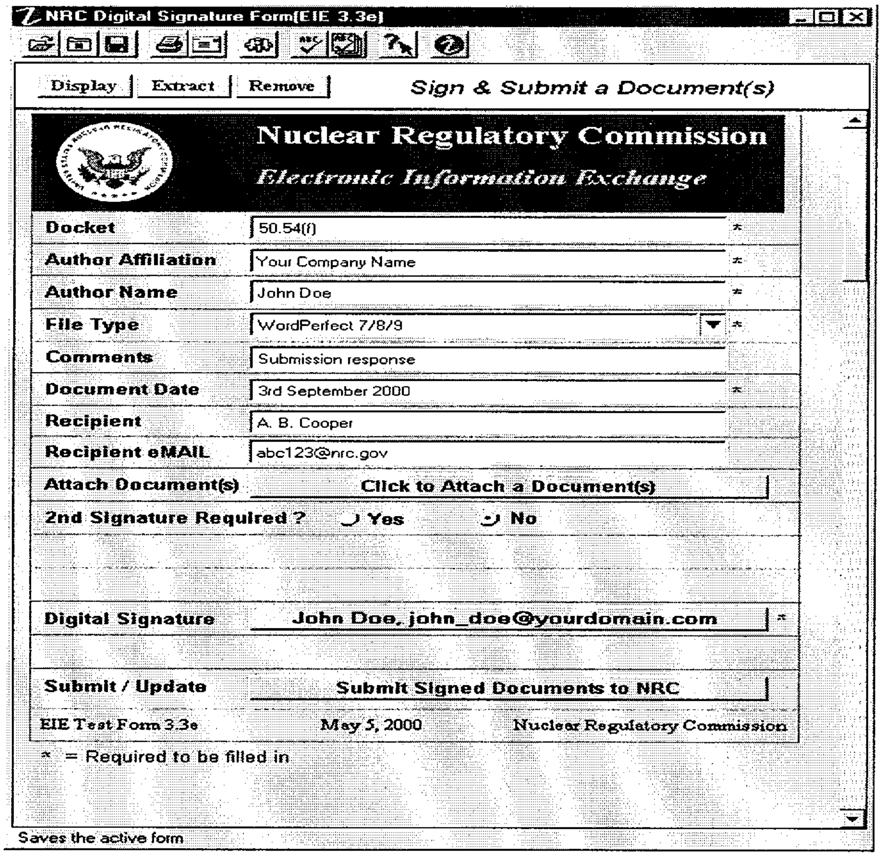
john_doe@yourdomain.com, John Doe, Digital ID Class 1 -- Netscape, Persona Not Validated, "www.verisign.com/repository/RPA Incorp. by Ref.,LIAB.LTD(c)98", VeriSign Trust Network, "VeriSign, Inc."

VeriSign Class 1 CA Individual Subscriber-Persona Not Validated, "www.verisign.com/repository/RPA Incorp. By Ref.,LIAB.LTD(c)98", VeriSign Trust Network, "VeriSign, Inc."

Figure 3-14: Digital Signature Viewer Dialog for Valid Signature

The viewer caption now changes to "Signature Is Valid."

Step 5: Sign the form by clicking on the **OK** button. The NRC EIE Form appears.



NRC Digital Signature Form[EIE 3.3e]

Sign & Submit a Document(s)

Nuclear Regulatory Commission

Electronic Information Exchange

Docket	50.54(f)	*
Author Affiliation	Your Company Name	*
Author Name	John Doe	*
File Type	WordPerfect 7/8/9	*
Comments	Submission response	
Document Date	3rd September 2000	*
Recipient	A. B. Cooper	
Recipient eMAIL	abc123@nrc.gov	
Attach Document(s)	Click to Attach a Document(s)	
2nd Signature Required ?	○ Yes ● No	
Digital Signature	John Doe, john_doe@yourdomain.com	*
Submit / Update	Submit Signed Documents to NRC	

EIE Test Form 3.3e   May 5, 2000   Nuclear Regulatory Commission

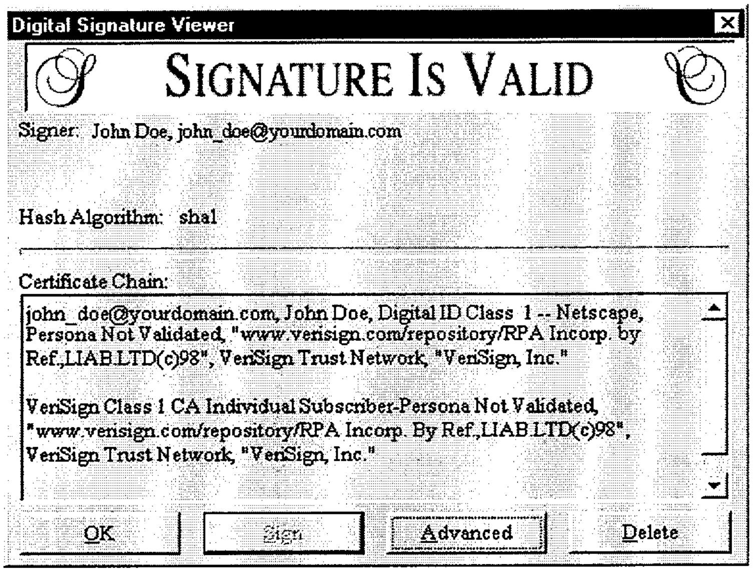
* = Required to be filled in

Saves the active form

Figure 3-15: Signed NRC EIE Form

The "Digital Signature" field on the form now displays the signer's name and e-mail address. After signing the form, it is ready to be submitted. Once the form is signed, it cannot be altered or modified. However, should a situation arise wherein a form is signed prematurely and additional material needs to be enclosed or material needs to be removed, the signature can be deleted to allow modification of the form's contents. To accomplish this, apply the following steps.

Step 1: Click on the **Click to Digitally Sign Document(s)** button on the form. This produces the Digital Signature Viewer.



Digital Signature Viewer

SIGNATURE IS VALID

Signer: John Doe, john_doe@yourdomain.com

Hash Algorithm: shal

Certificate Chain:

john_doe@yourdomain.com, John Doe, Digital ID Class 1 -- Netscape, Persona Not Validated, "www.verisign.com/repository/RPA Incorp. by Ref.,LIAB.LTD(c)98", VeriSign Trust Network, "VeriSign, Inc."

VeriSign Class 1 CA Individual Subscriber-Persona Not Validated, "www.verisign.com/repository/RPA Incorp. By Ref.,LIAB.LTD(c)98", VeriSign Trust Network, "VeriSign, Inc."

Figure 3-16: Digital Signature Viewer

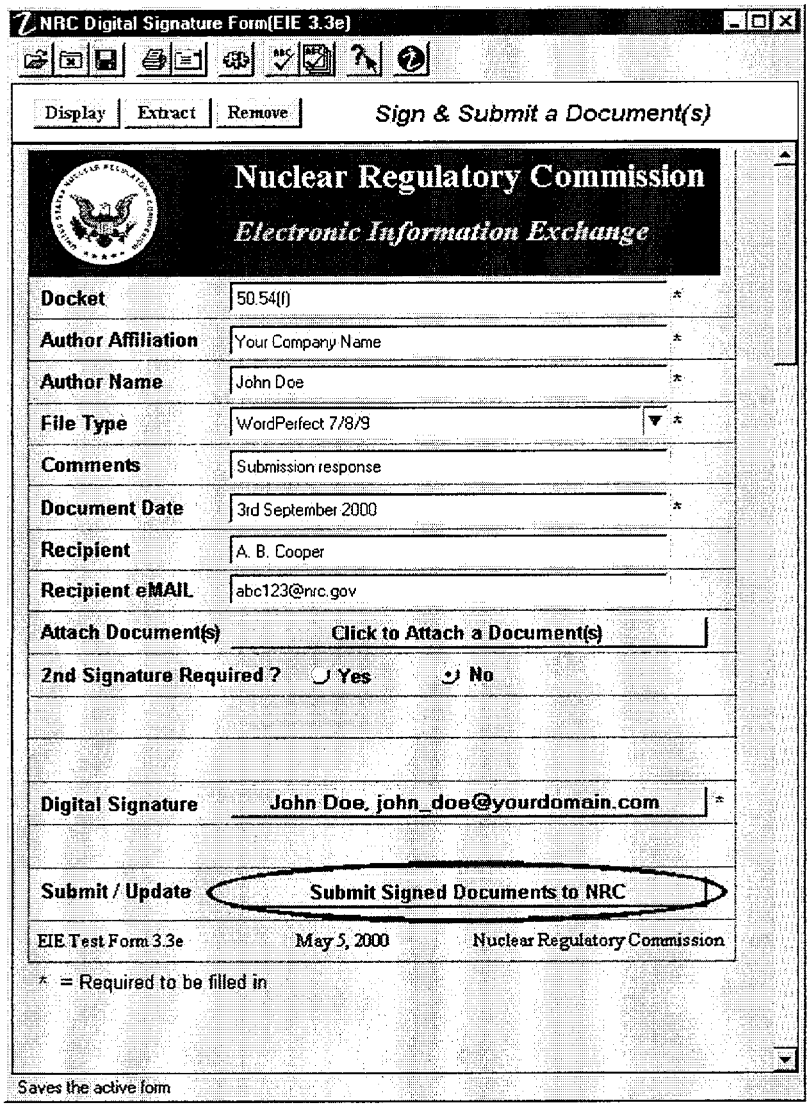
Step 2: The **Delete** button is highlighted. Click on the **Delete** button. This removes the signature.

Once the signature is removed, the form and its contents can be altered or modified as needed. When the necessary modifications are complete, the form should be re-signed.

3.6 How to Submit/Transmit Documents

Documents submitted to the NRC or transmitted from the NRC shall be deposited on the NRC EIE external server for retrieval. The external server exists outside the NRC firewall. In order to submit a form and its contents to the external server from a workstation, participants must follow these steps.

Step 1: With the form open, click on the **Submit Signed Documents to NRC** button. The cursor now changes to a black and white color wheel as the files are prepared and the Internet connection is attempted.


NRC Digital Signature Form(EIE 3.3e)
Display
Extract
Remove
Click to Attach a Document(s)
Submit Signed Documents to NRC
Saves the active form

Sign & Submit a Document(s)

Nuclear Regulatory Commission

Electronic Information Exchange

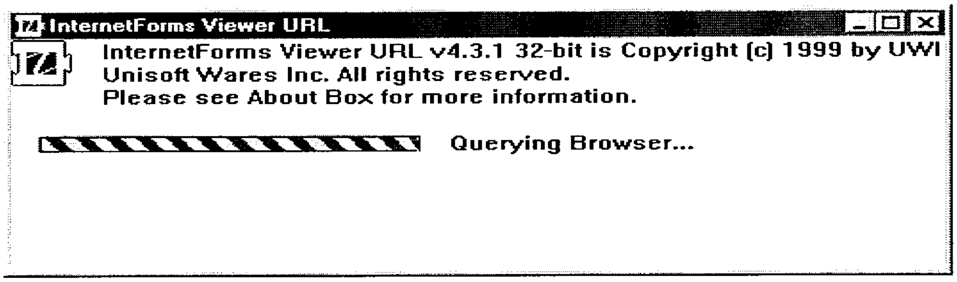
Docket	50.54(f) *
Author Affiliation	Your Company Name *
Author Name	John Doe *
File Type	WordPerfect 7/8/9 *
Comments	Submission response
Document Date	3rd September 2000 *
Recipient	A. B. Cooper
Recipient eMAIL	abc123@nrc.gov
Attach Document(s)	Click to Attach a Document(s)
2nd Signature Required ?	○ Yes ● No
Digital Signature	John Doe, john_doe@yourdomain.com *
Submit / Update	Submit Signed Documents to NRC

EIE Test Form 3.3e May 5, 2000 Nuclear Regulatory Commission

* = Required to be filled in

Figure 3-17: Submit Signed Documents to NRC

Step 2: Once the connection is established, the “Querying Browser” window appears and displays the progress of the file transmission.

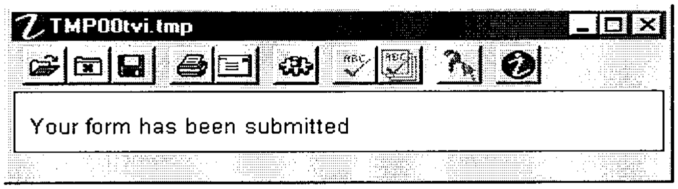


InternetForms Viewer URL v4.3.1 32-bit is Copyright (c) 1999 by UWI Unisoft Wares Inc. All rights reserved.
Please see About Box for more information.

Querying Browser...

Figure 3-18: Querying Browser

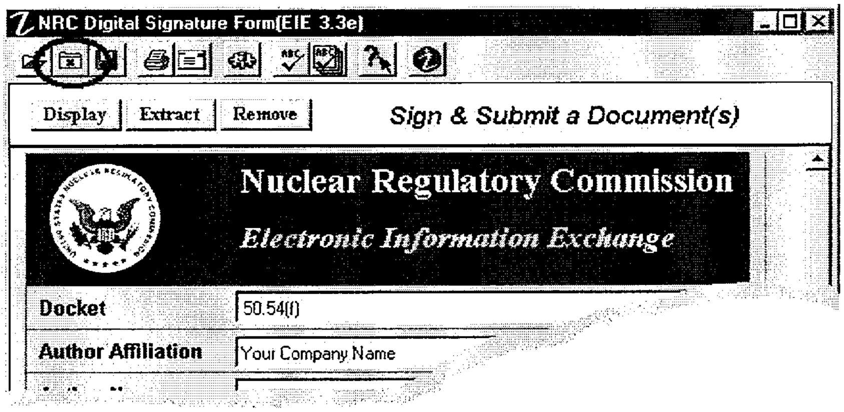
Step 3: Once the form is successfully submitted, the browser flashes a window that states “Your Form Has Been Submitted.”



Your form has been submitted

Figure 3-19: Successful Form Submittal Message

Step 4: Once the form has been submitted, close the form by clicking on the Close Form icon on the form toolbar. This returns you to the NRC EIE home page.

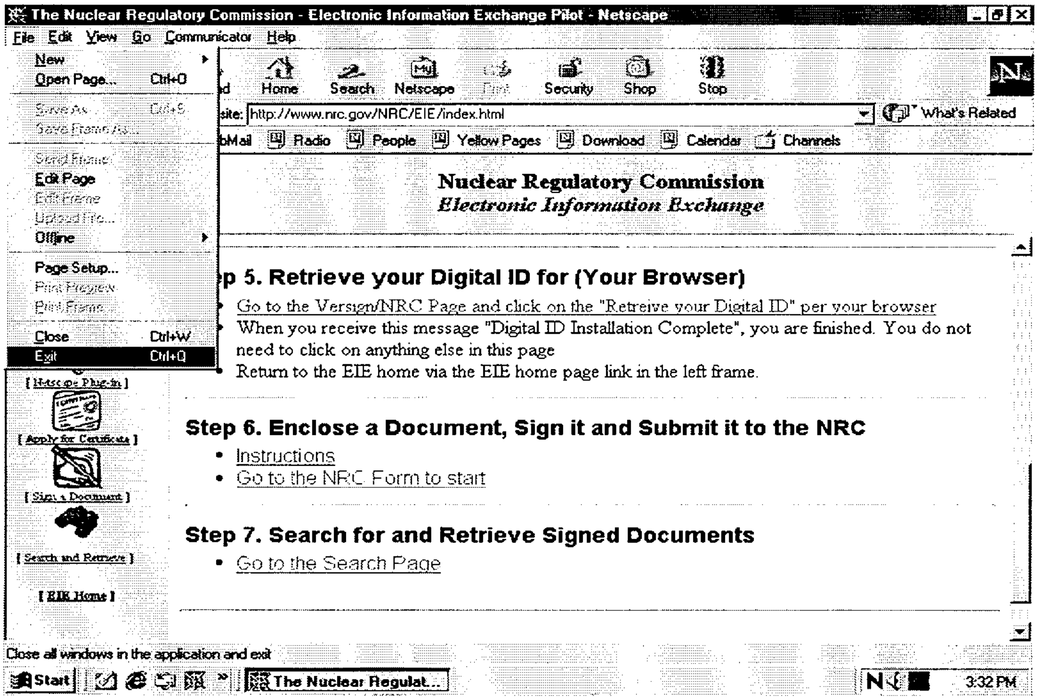

NRC Digital Signature Form[EIE 3.3e]
Display
Extract
Remove
Sign & Submit a Document(s)
Nuclear Regulatory Commission
Electronic Information Exchange

Docket 50.54(f)

Author Affiliation Your Company Name

Figure 3-20: Close Form

Step 5: Exit the home page and the browser by selecting **File** from the browser menu bar and click on **Exit** on the drop down menu.



Nuclear Regulatory Commission
Electronic Information Exchange

p 5. Retrieve your Digital ID for (Your Browser)

- Go to the Versign/NRC Page and click on the "Retreive your Digital ID" per your browser
- When you receive this message "Digital ID Installation Complete", you are finished. You do not need to click on anything else in this page
- Return to the EIE home via the EIE home page link in the left frame.

Step 6. Enclose a Document, Sign it and Submit it to the NRC

- Instructions
- Go to the NRC Form to start

Step 7. Search for and Retrieve Signed Documents

- Go to the Search Page

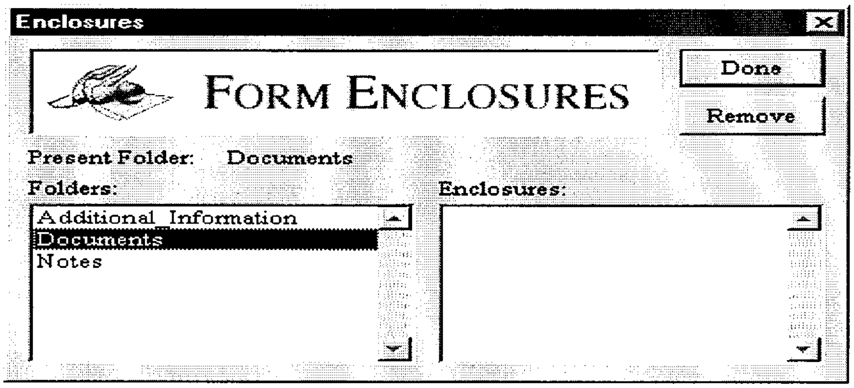
Close all windows in the application and exit

Figure 3-21: Exit EIE Home Page

3.7 How to Remove Documents

During the process of enclosing documents, a situation may arise wherein a document is enclosed in error. In such situations, the erroneously enclosed document may be removed. The process for removing a document is outlined below.

Step 1: With the form open, click on the **Remove** button. This opens the Enclosures dialog box for removing documents.



Present Folder: Documents

Figure 3-22: Remove Documents Dialog

Step 2: Highlight the folder on the left side of the dialog box containing the document to be removed. The document(s) within the folder are displayed on the right side of the dialog box.

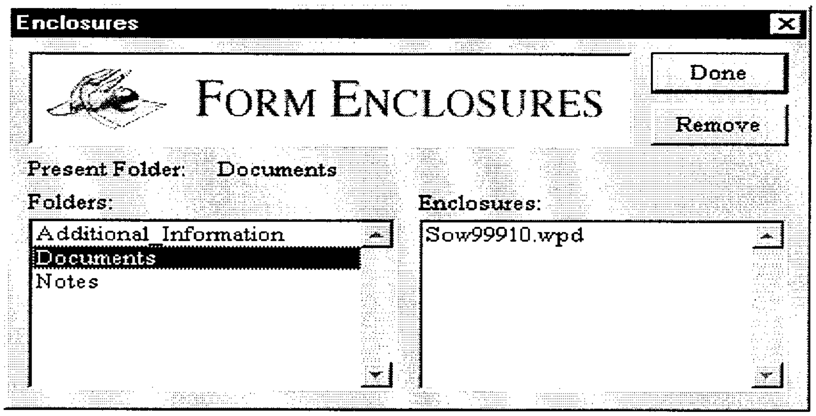


Figure 3-23: Document to be Removed

Step 3: Highlight the document to be removed and click on the **Remove** button. This produces a Remove Enclosure prompt.

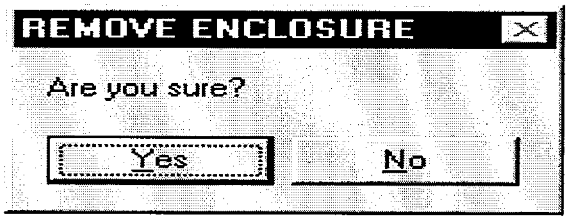


Figure 3-24: Remove Enclosure Prompt

Step 4: Click on the **Yes** button to remove the document.

4.0 HOW TO RETRIEVE DOCUMENTS

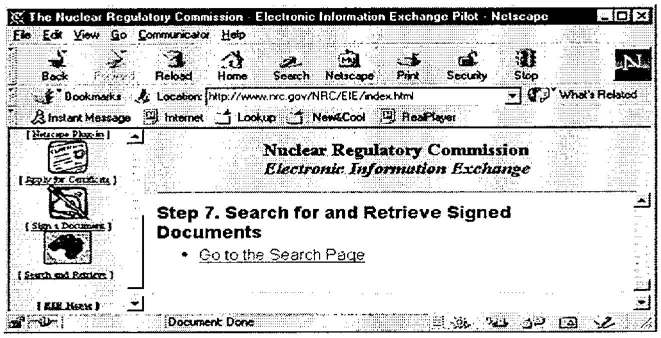
4.1 Introduction

When a form is submitted to the NRC external server, it is automatically date/time stamped at the time of receipt by the external server. This date/time stamp is intended to serve as the official date and time of receipt for both the NRC and it's customers. Intended recipients should receive an e-mail message providing notification of the submission and information necessary for it's retrieval such as; the author's name, author affiliation, document date, and docket number. Upon notification, recipients may access the external server and retrieve their documents. The steps involved in this process are as follows:

4.2 How to Search for Documents

Step 1: **Open** the Internet browser.

Step 2: Access the NRC EIE home page at http://www.nrc.gov/EIE/index.html. Once connected, go to Step 7, **Search for and Retrieve Signed Documents**.



Location: http://www.nrc.gov/NRC/EIE/index.html

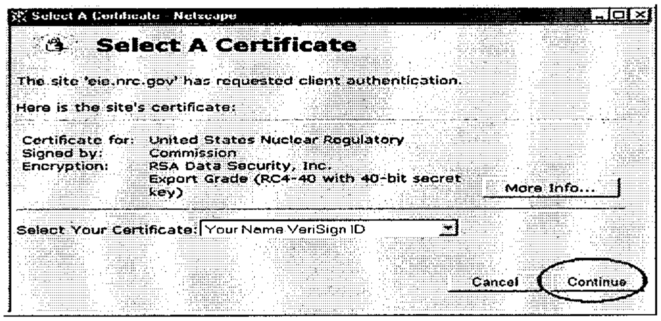
Nuclear Regulatory Commission
Electronic Information Exchange

Step 7. Search for and Retrieve Signed Documents

- Go to the Search Page

Figure 4-1: NRC EIE Home Page

Step 3: Click on the link, **Go to the Search Page**. The "Select a Certificate window appears.



Select A Certificate

The site 'eie.nrc.gov' has requested client authentication.

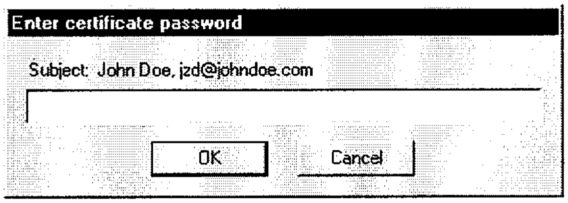
Here is the site's certificate:

Certificate for: United States Nuclear Regulatory
Signed by: Commission
Encryption: RSA Data Security, Inc.
Export Grade (RC4-40 with 40-bit secret key)

Select Your Certificate: Your Name VeriSign ID

Figure 4-2: Select a Certificate

Select your NRC issued certificate and click on the **Continue** button. The Password Entry dialog appears.

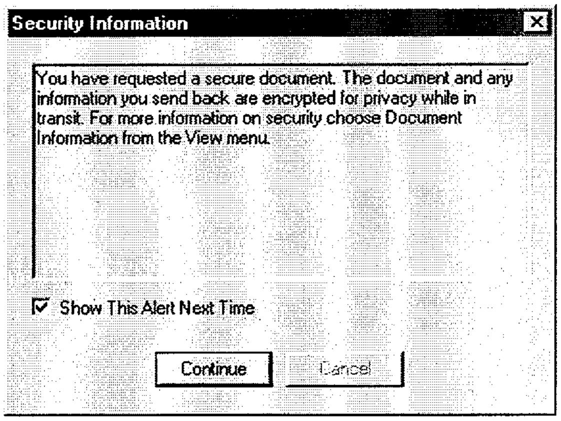


Enter certificate password

Subject: John Doe, jzd@johndoe.com

Figure 4-3: Netscape Password Dialog Box

Step 3: Enter your password for the Certificate Database and click on **OK**. You will be prompted to re-enter it for confirmation, click on the **OK** button. A Security Information window appears, click on **Continue**.



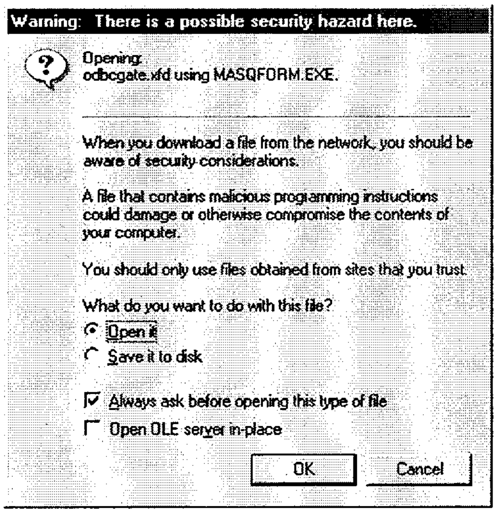
Security Information

You have requested a secure document. The document and any information you send back are encrypted for privacy while in transit. For more information on security choose Document Information from the View menu.

☑ Show This Alert Next Time

Figure 4-4: Security Information Window

Step 4: The Security Warning window now appears. Click on **OK** to continue.



Warning: There is a possible security hazard here.

Opening:
odbcgate.xfd using MASQFORM.EXE.

When you download a file from the network, you should be aware of security considerations.

A file that contains malicious programming instructions could damage or otherwise compromise the contents of your computer.

You should only use files obtained from sites that you trust.

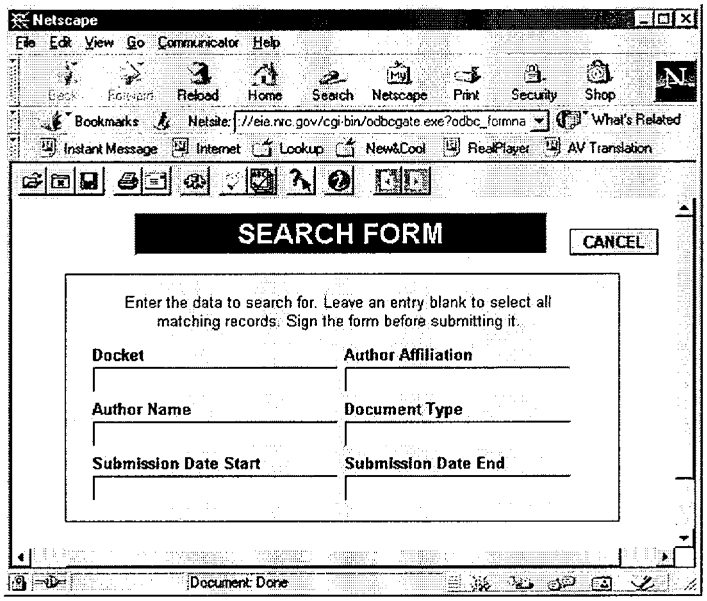
What do you want to do with this file?

● Open it
○ Save it to disk

☑ Always ask before opening this type of file
☐ Open OLE server in-place

Figure 4-5: Security Warning Window

This produces the Search Form window.


Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop
Bookmarks Netsite: //eie.nrc.gov/cgi-bin/odbcgate.exe?odbc_formna What's Related
Instant Message Internet Lookup New&Cool RealPlayer AV Translation
CANCEL
Document: Done

SEARCH FORM

Enter the data to search for. Leave an entry blank to select all matching records. Sign the form before submitting it.

Docket	Author Affiliation
Author Name	Document Type
Submission Date Start	Submission Date End

Figure 4-6: Search Form Dialog Window

Step 4: Enter search criteria.

The search criteria is used to search for the particular document sent to you. The search form allows searches to be performed on up to seven fields. Because search results provide matching records not only for the fields with information entered but also for the fields left blank, it is recommended that all available information be entered. The applicable search fields include Docket, Author Name, Author Affiliation, Recipient, Document Type, Submission Date Start, and Submission Date End.

Step 5: Once the search criteria has been entered, click on the **Sign Form And Search** button. The Digital Signature Viewer appears.

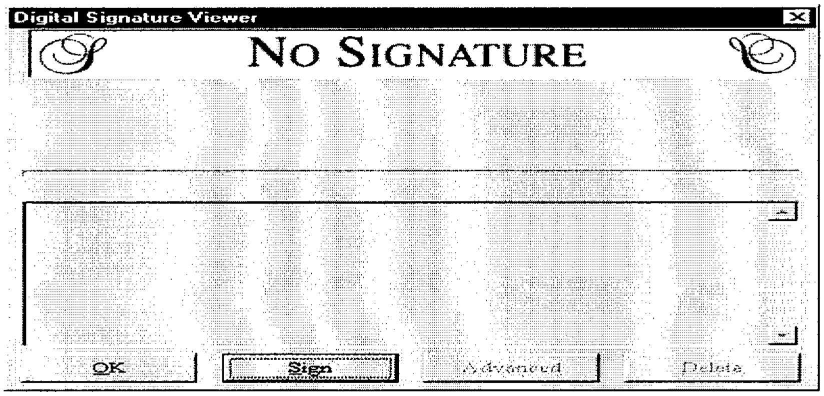
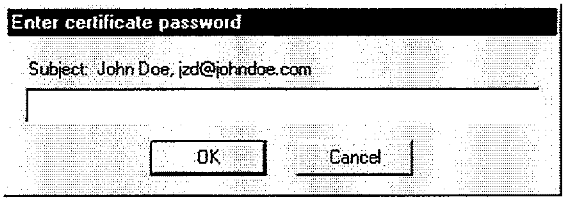


Figure 4-7: Digital Signature Viewer

Step 6: Click on the **Sign** button. This initiates a check for your Digital ID.

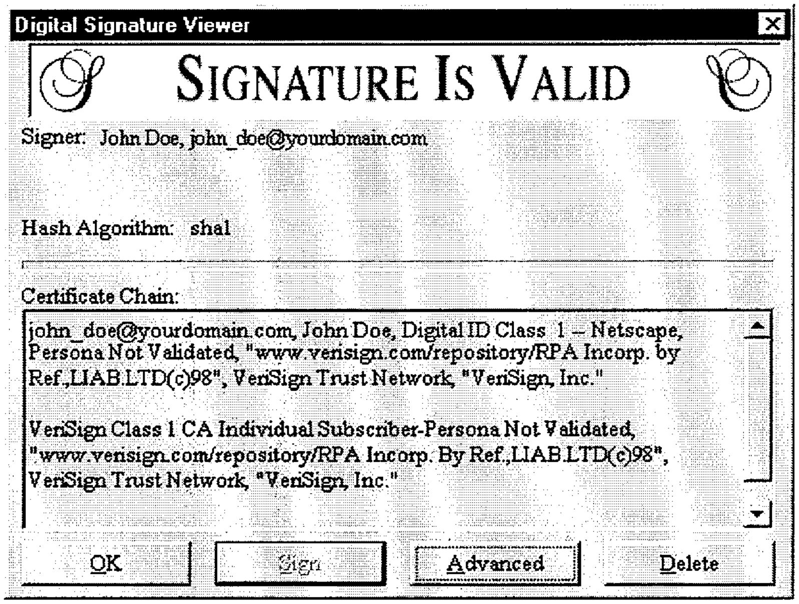


Subject: John Doe, jzd@johndoe.com

Figure 4-8: Netscape Password Dialog Box

Step 7: Netscape users are asked for their password for the Certificate Database.

Once a valid Digital ID is found, the Digital Signature Viewer appears with the Digital ID signaturing information.



Signer: John Doe, john_doe@yourdomain.com

Hash Algorithm: sha1

Certificate Chain:

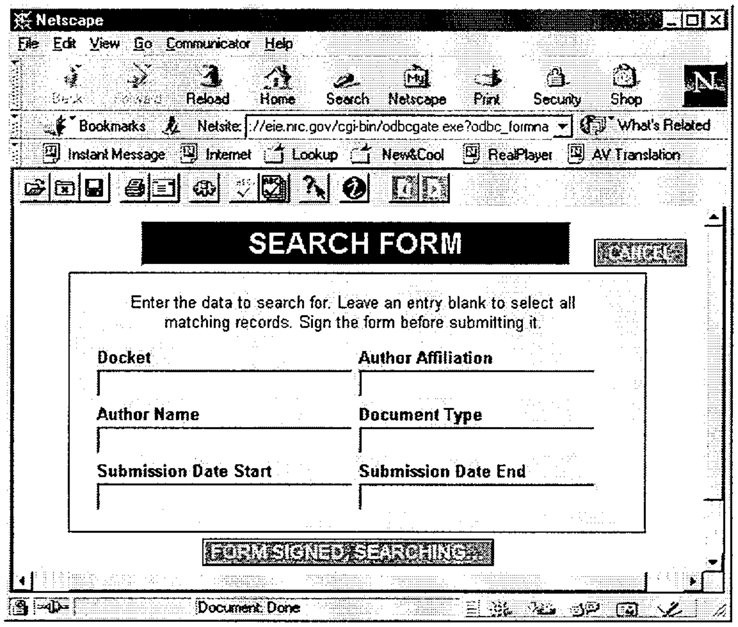
john_doe@yourdomain.com, John Doe, Digital ID Class 1 – Netscape, Persona Not Validated, "www.verisign.com/repository/RPA Incorp. by Ref.,LIAB.LTD(c)98", VeriSign Trust Network, "VeriSign, Inc."

VeriSign Class 1 CA Individual Subscriber-Persona Not Validated, "www.verisign.com/repository/RPA Incorp. By Ref.,LIAB.LTD(c)98", VeriSign Trust Network, "VeriSign, Inc."

Figure 4-9: Digital ID Signaturing Information

Click on the **OK** button. This action signs the Search Form.

The Search Form appears as signed and a message stating this is returned. At the same time, the **Sign Form And Search** button is transformed to **Form Signed, Searching...** .


Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop
Bookmarks Netsite: //eie.nrc.gov/cgi-bin/odbcgate.exe?odbc_formna What's Related
Instant Message Internet Lookup New&Cool RealPlayer AV Translation
CANCEL
FORM SIGNED, SEARCHING...
Document: Done

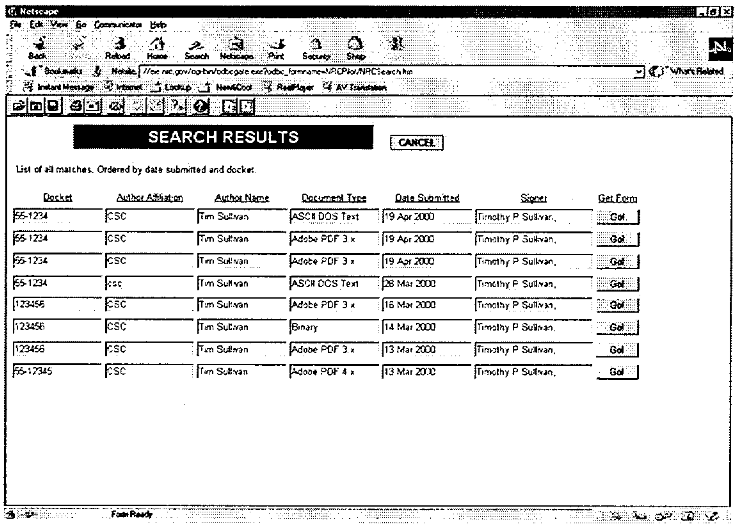
SEARCH FORM

Enter the data to search for. Leave an entry blank to select all matching records. Sign the form before submitting it.

Docket	Author Affiliation
Author Name	Document Type
Submission Date Start	Submission Date End

Figure 4-10: Signed Search Form

When the search is completed, the search results are returned listing the matching form or forms.


Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop
Bookmarks Netsite: //eie.nrc.gov/cgi-bin/odbcgate.exe?odbc_formname=NRCPilot/NRCSearch.htm What's Related
Instant Message Internet Lookup New&Cool RealPlayer AV Translation
CANCEL
Form Ready

SEARCH RESULTS

List of all matches. Ordered by date submitted and docket.

Docket	Author Affiliation	Author Name	Document Type	Date Submitted	Signer	Get Form
55-1234	CSC	Tim Sullivan	ASCII DOS Text	19 Apr 2000	Timothy P Sullivan,	Go!
55-1234	CSC	Tim Sullivan	Adobe PDF 3.x	19 Apr 2000	Timothy P Sullivan,	Go!
55-1234	CSC	Tim Sullivan	Adobe PDF 3.x	19 Apr 2000	Timothy P Sullivan,	Go!
55-1234	csc	Tim Sullivan	ASCII DOS Text	28 Mar 2000	Timothy P Sullivan,	Go!
123456	CSC	Tim Sullivan	Adobe PDF 3.x	16 Mar 2000	Timothy P Sullivan,	Go!
123456	CSC	Tim Sullivan	Binary	14 Mar 2000	Timothy P Sullivan,	Go!
123456	CSC	Tim Sullivan	Adobe PDF 3.x	13 Mar 2000	Timothy P Sullivan,	Go!
55-12345	CSC	Tim Sullivan	Adobe PDF 4.x	13 Mar 2000	Timothy P Sullivan,	Go!

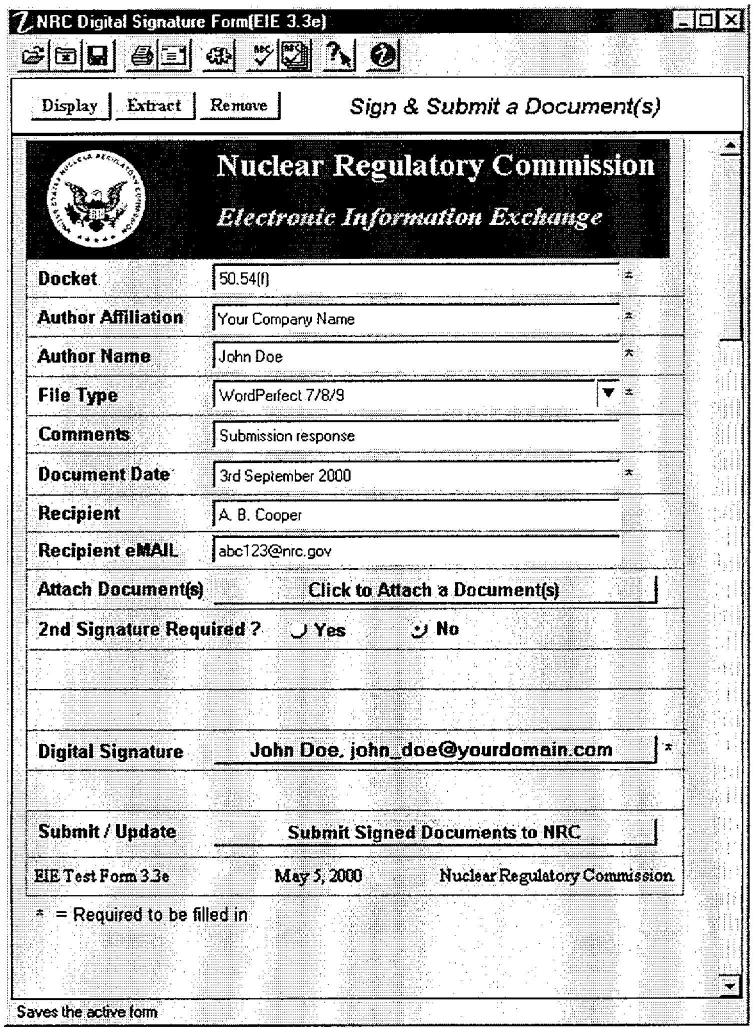
Figure 4-11: Search Results Dialog Window

The search results are returned in order of the date submitted and docket number. Once the list is provided, the form is ready to be retrieved. Locate the form to be retrieved and click on the GO! button on the right side of the listing. The submitted form is retrieved and displayed.

4.3 Authenticating the Form and Validating the Signature

Once the search for the appropriate form is complete and the form sought is digitally signed, the authentication and validation processes must be followed as outlined below.

Step 1: Once the form appears, click on the button displaying the sender's name and e-mail address to validate the signature and authenticate the form.


NRC Digital Signature Form(EIE 3.3e)
Display
Extract
Remove
Sign & Submit a Document(s)
Nuclear Regulatory Commission
Electronic Information Exchange
Click to Attach a Document(s)
Submit Signed Documents to NRC

Docket	50.54(f) *
Author Affiliation	Your Company Name *
Author Name	John Doe *
File Type	WordPerfect 7/8/9 *
Comments	Submission response
Document Date	3rd September 2000 *
Recipient	A. B. Cooper
Recipient eMAIL	abc123@nrc.gov
Attach Document(s)	Click to Attach a Document(s)
2nd Signature Required ?	○ Yes ● No
Digital Signature	John Doe. john_doe@yourdomain.com *
Submit / Update	Submit Signed Documents to NRC

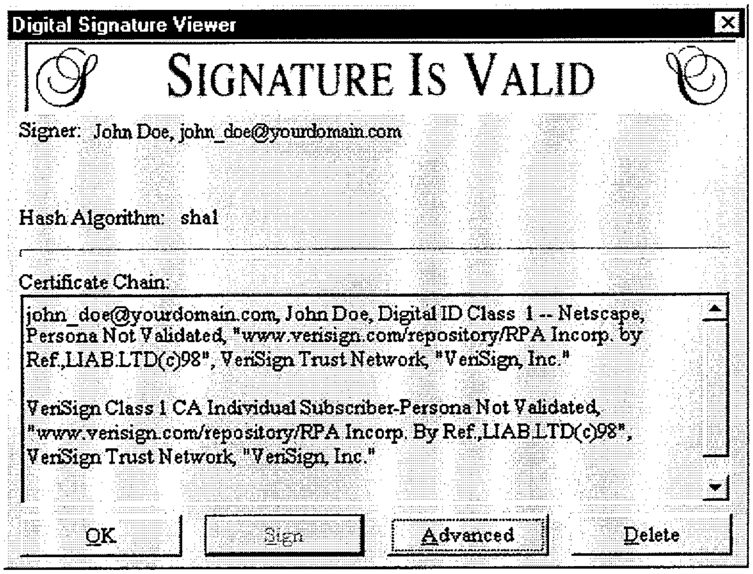
EIE Test Form 3.3e May 5, 2000 Nuclear Regulatory Commission

* = Required to be filled in

Saves the active form

Figure 4-12: Submitted NRC EIE Form

The Digital Signature Viewer appears.



SIGNATURE IS VALID

Signer: John Doe, john_doe@yourdomain.com

Hash Algorithm: shal

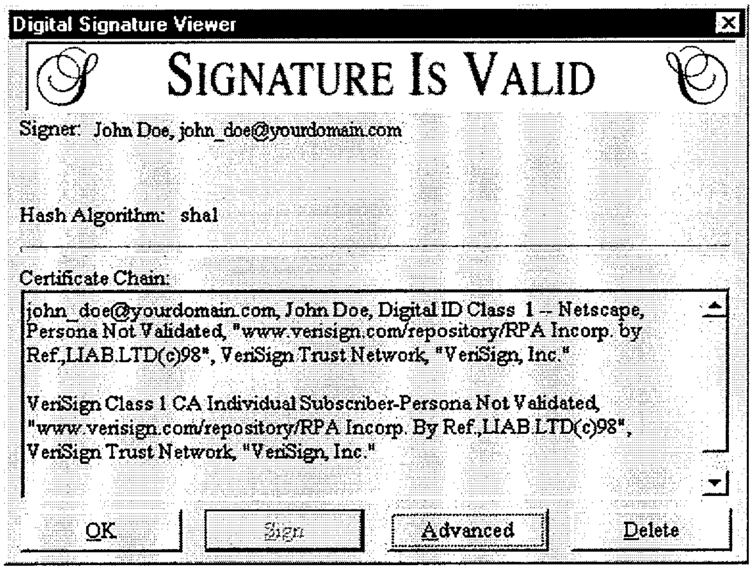
Certificate Chain:

john_doe@yourdomain.com, John Doe, Digital ID Class 1 -- Netscape, Persona Not Validated, "www.verisign.com/repository/RPA Incorp. by Ref.,LIAB.LTD(c)98", VeriSign Trust Network, "VeriSign, Inc."

VeriSign Class 1 CA Individual Subscriber-Persona Not Validated, "www.verisign.com/repository/RPA Incorp. By Ref.,LIAB.LTD(c)98", VeriSign Trust Network, "VeriSign, Inc."

Figure 4-13: Digital Signature Viewer – Signature is Valid

If the form has not been altered, the viewer appears with a message stating that the "Signature Is Valid" thus validating the signature and authenticating the form. The window also displays information about the signer.



SIGNATURE IS VALID

Signer: John Doe, john_doe@yourdomain.com

Hash Algorithm: shal

Certificate Chain:

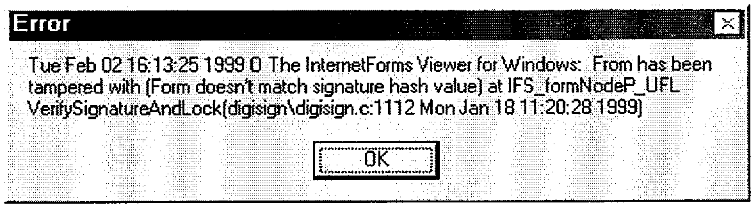
john_doe@yourdomain.com, John Doe, Digital ID Class 1 -- Netscape, Persona Not Validated, "www.verisign.com/repository/RPA Incorp. by Ref.,LIAB.LTD(c)98", VeriSign Trust Network, "VeriSign, Inc."

VeriSign Class 1 CA Individual Subscriber-Persona Not Validated, "www.verisign.com/repository/RPA Incorp. By Ref.,LIAB.LTD(c)98", VeriSign Trust Network, "VeriSign, Inc."

Figure 4-14: Digital Signature Viewer – Signature is Valid

Step 3: After validating the signature, click on the **OK** button to return to the form. You may then proceed to retrieve the enclosed documentary material.

However, if the form has been altered, an error message appears stating that the **"form has been tampered with (form does not match signature hash value)."**



```
Tue Feb 02 16:13:25 1999 0 The InternetForms Viewer for Windows:  From has been
tampered with (Form doesn't match signature hash value) at IFS_formNodeP_UFL
VerifySignatureAndLock(digisign\digisign.c:1112 Mon Jan 18 11:20:28 1999)
```

Figure 4-15: Altered Form Error Message

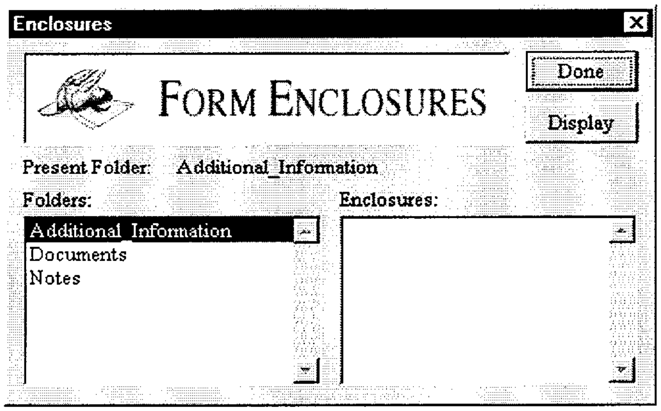
If the form has been altered, click on the **OK** button to return to the form and promptly notify the LRAA and delete the file. The LRAA will notify the sender of the alteration and request re-submission.

4.4 Document Access and Retrieval

After locating the form and validating the signature, participants can proceed to access, view, and retrieve any documents enclosed in the form. Enclosed documentary material can be viewed using the form's display function or retrieved using the form's extract function. The steps involved in performing each function are listed below.

Displaying Documents

Step 1: With the form open, click on the **Display** button on the form. The "Enclosures" dialog window appears.



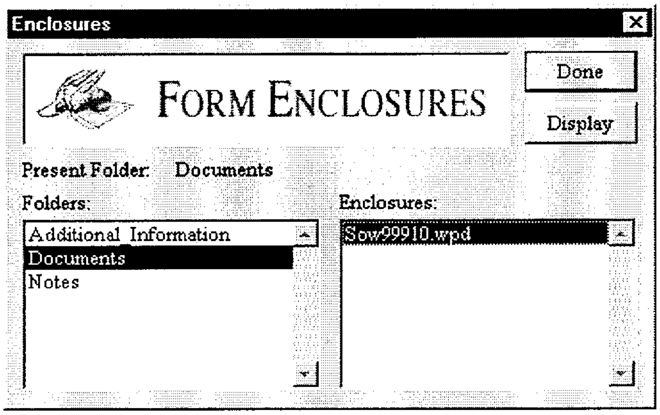
Present Folder: Additional_Information

Folders:
Additional_Information
Documents
Notes

Enclosures:

Figure 4-16: Enclosures Dialog Window

Step 2: Select the folder containing the documents to be viewed by clicking the folder name in the folder window. The enclosed document file names now appear on the right side of the dialog box in the "Enclosures" window.



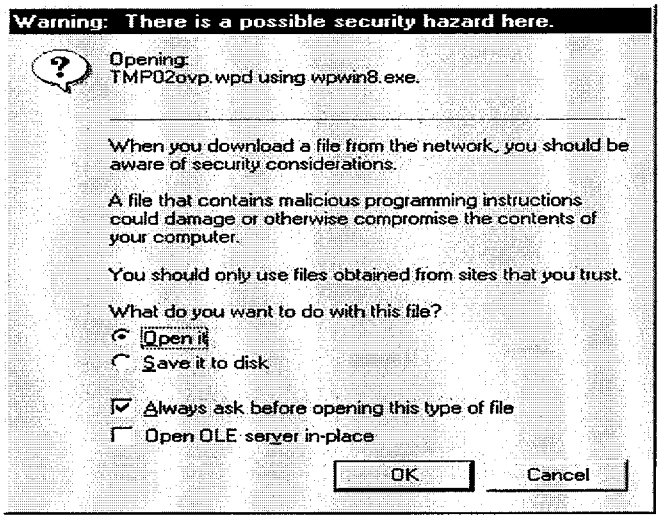
Present Folder: Documents

Folders:
Additional Information
Documents
Notes

Enclosures:
Sow99910.wpd

Figure 4-17: Display Enclosures Window

Step 3: Highlight the document file name and click on the **Display** button. This invokes the browser and produces a Security Warning Dialog.


Warning: There is a possible security hazard here.

Opening:
TMP02ovp.wpd using wpwin8.exe.

When you download a file from the network, you should be aware of security considerations.

A file that contains malicious programming instructions could damage or otherwise compromise the contents of your computer.

You should only use files obtained from sites that you trust.

What do you want to do with this file?
● Open it
○ Save it to disk

☑ Always ask before opening this type of file
□ Open OLE server in-place

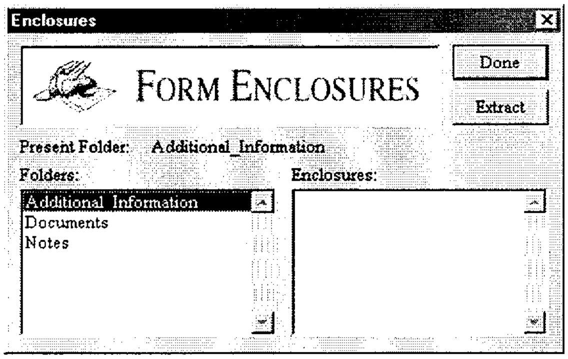
Figure 4-18: Warning Dialog Window

Step 4: Click on the OK button to open the document.

Retrieving Documents

In order to retrieve documents from the external server to your workstation or local network, participants can use the form's extract function. The process to extract a document is the reverse of the process to enclose a document. The steps involved in the extraction process are as follows.

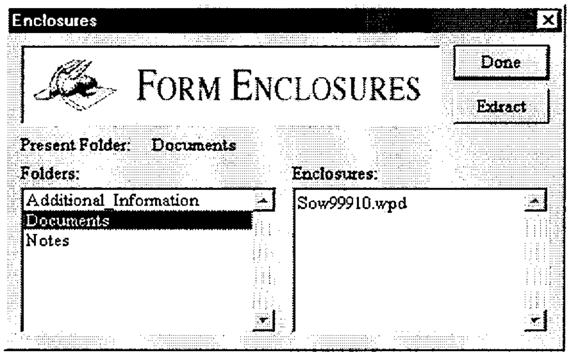
Step 1: With the form open, click on the **Extract** button. The "Enclosures" dialog box appears.



Present Folder: Additional_Information

Figure 4-19: Enclosures Dialog Window to Extract Documents

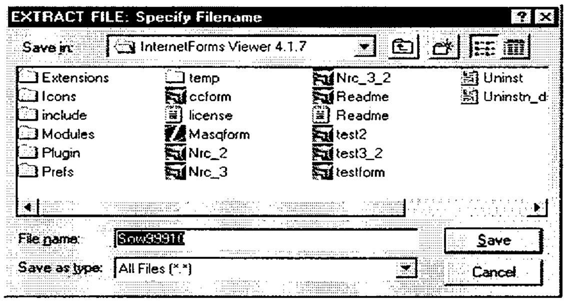
Step 2: Click on the folder name containing the document(s) to be extracted in the folder window on the left side of the dialog window. The enclosed document file name(s) appears in the "enclosures" window on the right side of the dialog box.



Present Folder: Documents

Figure 4-20: Enclosure Dialog with Document Highlighted

Step 3: Highlight the document file name and click on the **Extract** button. The Extract File window is now open.



Save in: InternetForms Viewer 4.1.7

File name: Sow9991(

Save as type: All Files (*.*)

Figure 4-21: Extract File Window

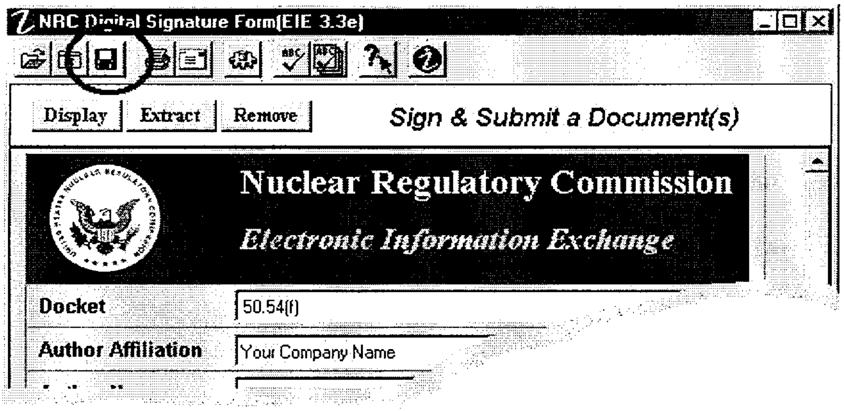
Step 4: Navigate to the local or network drive and folder or subdirectory where you intend to store the document file. Once there, click the **Save** button to extract the document from the form and to place it in the chosen folder or subdirectory. You are then returned to the Enclosure dialog. If there are multiple documents to extract, repeat this process until all have been extracted.

Step 5: When all documents have been extracted, click on the **Done** button on the Enclosure dialog box. This returns you to the form.

4.5 Deleting and Saving Forms

Participants should not attempt to delete or remove forms from the external server since forms may be intended for multiple recipients. The responsibility for file maintenance resides with the NRC EIE system administrator. If a form or form package is uploaded to the external server by mistake, participants should notify the LRAA at LRAA@nrc.gov. If a participant wishes to retain a copy of the form, follow the steps listed below.

Step 1: Click on the **Save** icon on the form's menu bar.

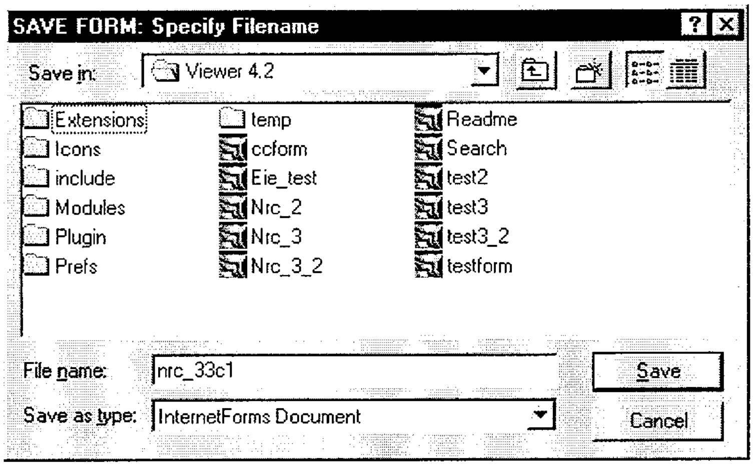

NRC Digital Signature Form(EIE 3.3e)
Display
Extract
Remove
Sign & Submit a Document(s)
Nuclear Regulatory Commission
Electronic Information Exchange

Docket: 50.54(f)

Author Affiliation: Your Company Name

Figure 4-22: NRC EIE Form with Save Function Highlighted

This opens the Save Form window.



SAVE FORM: Specify Filename

Save in: Viewer 4.2

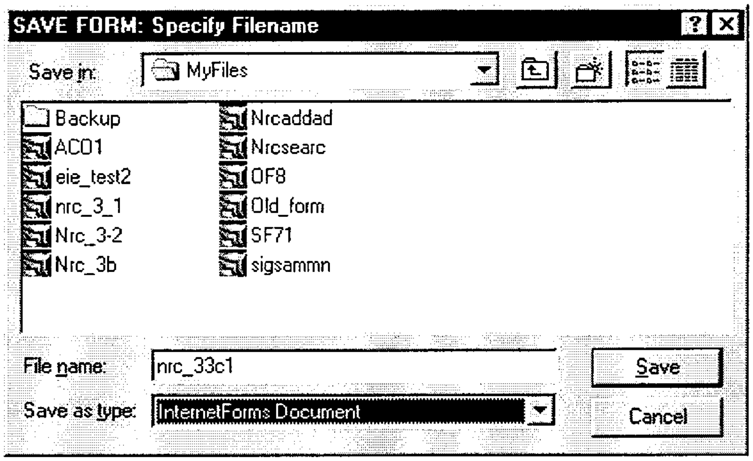
File name: nrc_33c1

Save as type: InternetForms Document

Figure 4-23: Save Form Window

Step 2: With the Save Form window open, specify a file name.

Step 3: Then, navigate to the appropriate drive, folder, or directory in which to save the file.



SAVE FORM: Specify Filename

Save in: MyFiles

File name: nrc_33c1

Save as type: InternetForms Document

Figure 4-24: Save Form Window

Step 4: Click on the <u>S</u>ave button. All forms are saved with the file extension ".xfd."

Statement of Liability

The provision of an electronic information exchange system by the NRC for the purposes of submitting and transmitting documentary material is based on the terms and conditions outlined below. Those who use the NRC's EIE system do so of their own accord. The exchange of information shall be conducted in good faith among the parties participating. The NRC shall have no responsibility to warrant the authenticity of the information exchanged nor to validate the identity of those involved in the exchange. The NRC shall not be liable in any actions arising from transactions among parties participating in the EIE process in accordance with the authorities and statements of guidance listed below.

□ Relevant Federal Regulations

The use of the NRC EIE Public Certification Services are subject to various U.S. Federal and State criminal laws, which may include but are not limited to: 18 U.S.C. § 1030 (Computer Fraud and Abuse Act of 1986), 18 U.S.C. § 1343 (Federal Wire Fraud Act), 18 U.S.C. § 2701 (Unlawful Access to Stored Communications - The Electronic Communications Privacy Act of 1986), and 18 U.S.C. § 1029 (Fraud and Related Activity in Connection with Computers).

□ Exclusion of Certain Elements of Damages

In no event shall any issuing authority or NRC be liable for any indirect, special, incidental, or consequential damages, or for any loss of profits, loss of data, or other indirect, consequential, or punitive damages arising from or in connection with the use, delivery, license, performance, or nonperformance of certificates, digital signatures, or any other transactions or services offered or contemplated by the NRC, even if such issuing authorities or NRC, or both, have been advised of the possibility of such damages.

□ Subscriber Liability to Relying Parties

Without limiting other subscriber obligations, subscribers are liable for any misrepresentations they make in certificates to third parties who, having verified one or more digital signatures with the certificate, reasonably rely on the representations contained therein.

Glossary of Terms

Access Control List (ACL)

A specific list of individuals or groups that are allowed access to specific areas of the NRC EIE external server.

Certificate Authority (CA)

The trusted authority that creates, assigns, tracks, maintains, and publishes certificates.

Certificate Database

The file which contains your Digital ID certificate within the Netscape Navigator or Communicator browser.

Challenge Phrase

A set of numbers and/or letters that are chosen by a certificate applicant, communicated to the issuing authority with a certificate application, and used by the issuing authority to authenticate the subscriber for various purposes.

Digital ID Certificates

A special data structure that contains a user's unique identification, the user's public key, and some parameters related to the validity of the certificate such as the date of expiration. Digital certificates, with public keys, are maintained openly in a directory in the possession of a certificate or certifying authority (currently VeriSign, Inc.).

Digital Signatures

A digital signature is a checksum which is the result of the application of a secret key and algorithm to a message. As a result, the digital signature is not constant; that is, it always depends on the bit values of the document that it signs. Upon receipt of the document, the digital signature is re-created and compared to the transmitted digital signature. If the signatures match, the sender is authenticated and the document integrity is assured. A non-match indicates that either the document was altered or that the signature is not that of the expected sender.

Encryption Strength

The strength of the encryption depends on the length of the key used. The length of the key is measured in "bits." Generally, longer keys are stronger than shorter keys. Key size ranges from 512 bits to 1024 bits.

Key Generation

The process of creating a private key during certificate application whose corresponding public key is submitted to the Certificate Authority for validation.

Key Pair

A set of encrypted keys composed of a private key and a corresponding public key. The private key is known only to you and is not communicated to the Certificate Authority.

Local Registration Authority (LRA)

NRC staff who identify candidates to be certificate holders and vouches for the binding between public keys and certificate holder identities.

Local Registration Authority Administrator (LRAA)

NRC staff who receives and reviews certificate requests, approves or disapproves certificate requests, notifies the Certification Authority of approve/disapprove decisions, and performs review of requirements related to the digital signatures.

Portable Document Format (PDF)

A standard to make the interchange of formatted documents between differing computing environments as reliable as possible. It is designed to ensure the integrity of the document being interchanged regardless of the computer, operating system, or application software used to create the original document.

Private Key

A mathematical key (kept secret by the holder) used to create digital signatures and, depending upon the algorithm, to decrypt messages or files encrypted (for confidentiality) with the corresponding public key.

Public Key

A mathematical key that can be made publicly available and which is used to verify signatures created with its corresponding private key. Depending on the algorithm, public keys are used to encrypt messages or files which can then be decrypted with the corresponding private key.

Public Key Infrastructure (PKI)

A system for publishing the public-key values used in public-key cryptography. There are two operations common to all PKIs. *Certification* is the process of binding a public-key value to an individual, organization or other entity, or even to some other piece of information, such as a permission or credential. *Validation* is the process of verifying that a certification is still valid.

Secure Hypertext Transfer Protocol (HTTP-S)

HTTP-S provides secure communication mechanisms between an HTTP client/server pair in order to enable spontaneous commercial transactions for a wide range of applications. It provides a flexible protocol that supports multiple orthogonal operation modes, key management mechanisms, trust models, cryptographic algorithms, and encapsulation formats through option negotiation between parties for each transaction.

Secure Sockets Layer (SSL3)

A protocol designed to enable encrypted, authenticated communications across the Internet. URLs that begin with “https” indicate that an SSL connection will be used. In an SSL connection, each side of the connection must have a

	Security Certificate. SSL3 includes three things; privacy, authentication, and message integrity.
Time Stamp	A notation that indicates (at least) the correct date and time of an action, and identity of the person or device that sent or received the time stamp.
Uniform Resource Locator (URL)	A standardized device for identifying and locating certain records and other resources located on the World Wide Web.

Appendix A. Digital Certificate Request Confirmation

From: <jas1@nrc.gov>
To: john_smith@labat.com
Date: Thu, Aug 26, 1999 8:00 AM
Subject: Digital ID request confirmation

Dear John Smith,

Thank you for requesting a Digital ID. Your administrator is processing your request, and will notify you when your Digital ID is ready.

If you have questions about your application, please contact your Administrator by replying to this e-mail message.

Appendix B. Digital Certificate Request Disapproval

From: <jas1@nrc.gov>
To: TWFN_DO.twf2_po(TPS)
Date: Fri, Aug 27, 1999 8:27 AM
Subject: Cannot Process Digital ID Request

Dear JOHN Q PUBLIC

Your Administrator was not able to approve your Digital ID/certificate request based on the information you provided.

You may receive another e-mail detailing the specific reasons why your Administrator could not issue your Digital ID. If you have questions, please contact your Administrator by replying to this e-mail message.

Appendix C. Digital Certificate Approval Notification

From: <jas1@nrc.gov>
To: john_smith@labat.com
Date: Fri, Aug 27, 1999 9:22 AM
Subject: Your Digital ID is ready

Dear John Smith,

Your Administrator has approved your Digital ID request. To assure that someone else cannot obtain a Digital ID that contains your personal information, you must retrieve your Digital ID from a secure web site using a unique Personal Identification Number (PIN). You can retrieve your Digital ID by following these simple steps:

Step 1: Visit the Digital ID retrieval web page. If your Administrator has set up a customized location for retrieving your Digital ID, you should visit the URL specified by your Administrator. Otherwise, you can retrieve your ID at

https://onsite.verisign.com/USNuclearRegulatoryCommissionADDOCIO/index.html

Step 2: In the form, enter your Personal Identification Number (PIN):

Your PIN is: XXXXXXXXX

Step 3: Follow the instructions on the page to complete the installation of your Digital ID.

If you have any questions or problems, please contact your Administrator by replying to this e-mail message.

UNITED STATES NUCLEAR REGULATORY COMMISSION