Digital ID Certificates Guide

January 21, 2009

Revision 2

Table of Contents

<u>Note</u>: .To see this instructional guide in video format, go to the NRC's "Obtain a Digital ID Certificate" website (http://www.nrc.gov/site-help/e-submittals/apply-certificates.html). Under "Related Links", select any of the three video links displayed: **Digital ID Certificate Video**, **Exporting a Certificate Video** or **Importing a Certificate Video**.

Also visit the NRC's "Electronic Submittal" website (http://www.nrc.gov/site-help/e-submittals.html). Under "Submittal Instructions", select the **How to Submit Documents Video Instruction** link and the **Install the Workplace Forms Viewer Video Instruction** link

You may also right-mouse click on the Video Instruction link and save these videos to your computer, then open the video file.

1. Introduction

The U.S. Nuclear Regulatory Commission (NRC) requires individuals and organizations to have digital ID certificates in order to submit and/or view documents electronically. The Electronic Information Exchange (EIE) system was the first NRC system requiring digital IDs. This system supports several document submission forms used by different program areas at the NRC. The NRC is developing more applications, which will require digital certificates for access.

Digital ID certificates are stored in the user's web browser such as Microsoft's Internet Explore web browser.

The NRC uses client style digital certificates issued through VeriSign Inc. The digital certificates enable NRC's users to establish secure encrypted communications between the users' PC and the NRC's application servers.   The NRC uses digital certificates in conjunction with logins and/or special access lists to control access to some applications. The NRC uses digital certificates for digital signing and to enable encrypted communications using a two-key security technology and a public key infrastructure. Digital certificates provide an added level of protection against electronic fraud and malicious Internet based communications. Use of digital certificates makes it much more difficult for someone to electronically steal another person's login and password and transmit false or misleading information.

2. NRC's Use of Digital ID Certificates

Three different EIE programs require NRC customers to use digital ID certificates. People submitting documents to the NRC must determine which program will meet their needs and contact this program's staff to get approval to participate. The three program areas are:
   1. Criminal History Program
   2. Adjudicatory Proceedings
   3. General Form

The Criminal History Program supports nuclear power plant requests for FBI background investigations of their staff. Fingerprints and other personal data are transmitted via this program. Participants in this program need to be sponsored by a nuclear power plant and must be included on the Criminal History Program's access list.

The Adjudicatory Proceedings Program (which involves any case being brought before the NRC) uses digital ID certificates and various access lists to enable hearing participants to submit and view appropriate hearing materials. Access rights to hearing materials are controlled based upon the sensitivity of documents and other factors judged appropriate. Documents associated with various adjudicatory hearings will have lists of people who may have various access rights to hearing documents.

The General Form Program is less restrictive and is functionally like an electronic mailbox for incoming documents from various individuals representing many public and corporate entities. This form allows people to submit digitally signed documents to the NRC for a variety of purposes.

3. Public Key Infrastructure Security – What is it?

NRC-issued VeriSign certificates use a Managed Public Key Infrastructure (MPKI). A Public Key Infrastructure (PKI) enables users to securely and privately exchange information through the use of a public and private cryptographic key pair that is obtained and shared through a trusted authority. PKI provides a digital certificate that can identify an individual, device, or organization and directory services that can store, add, and revoke certificates. PKI is an enabler of trust that provides strong user identification, confidential communication, data integrity, and evidence for non-repudiation among individuals who may or may not have had prior knowledge of each other. Non-repudiation provides a proof-of-participation in an action or transaction by establishing that a user's private key was used to digitally sign an electronic business transaction. The trust that PKI facilitates is enterprise-wide through distinct yet integrated policies and technology components. These policies and components explicitly identify and determine the roles, responsibilities, constraints, range of use, and services available.

Mathematically related key pairs (a public key and a private key) are generated through the use of PKI technology. While the users' private key is safeguarded, their public key is linked to identifying information in a digitally signed public key certificate, certifying their ownership of both public and private keys. The certificate and the keys are used in systems and applications to represent the user or individual identified by the certificate. A user must have one current key pair for encryption and decryption, and a second key pair for digital signature and signature verification.

The public key can be accessed by anyone. Only the person to whom the private key is issued has knowledge of this key; the private key is never revealed or transmitted. What one key in the pair encrypts, only the other key can decrypt. The keys are mathematically related in such a way that guessing one key from the other is almost impossible. For example, a user (Bob) can send a message to another user (Carol) by encrypting the message with "Carol's" public key because only "Carol" holds the private key to decrypt it. For authenticity (digital signature), "Bob" can send "Carol" a message encrypted with his private key. "Carol" can be certain the message came from "Bob" because the message can be decrypted only by using "Bob's" public key.   The identity of "Bob" is verifiable because only "Bob" has access to his private key.

A digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document.   Besides being easily transportable, the digital signature ensures that the content of the message or document is unchanged. When time-stamped, the ability to ensure that the original signed message arrived means that the sender cannot easily repudiate it later.

Certification Authorities (CAs) represent the people, processes, and tools to create digital certificates that securely bind the names of users to their public keys. The following four parties rely on the appropriate level of trust with respect to the creation and use of public key certificates:
① The individual subscriber or entity identified by the certificate,
② The Certification Authority who issues the certificate,
③ The Registration or Validation Authority that provides certificate validation services in certain implementations, and
④ The Relying Party (company, agency or individual) relying on the certificate.

As long as users trust a CA and the CA's policies for issuing and managing certificates, the users can trust certificates issued by the CA. The CA investigates individuals and verifies their identity, binding that identity to the public key and verifying that the individual has the

private key. Levels of trust are placed on the level of identification and verification required by the certificate level (e.g. low, moderate, high).

4. Overview of the steps to get a Digital ID Certificate from NRC

There are three steps to get a VeriSign Digital ID from the NRC:
① Request an NRC Approval Code from the associated NRC program staff,
② Enroll for your Digital ID certificate on-line using the NRC Approval code, and
③ Install your Digital ID certificate in your personal computer's web browser.

To submit documents to the NRC, you must request inclusion in a program and be given a NRC digital ID approval code. This code is needed when you enroll for your digital ID. The first step in the digital ID request process is to contact the appropriate NRC program area person. Some of the NRC's electronic document submittal programs are set up for very specific groups of people with specialized document transmission needs. To open forms and submit documents for NRC's Criminal History program or NRC's Adjudicatory Proceedings program, you must have a digital ID and you must be included on a computerized access list for the program.

After you have received the NRC digital ID approval code from the appropriate NRC authority, you are now ready to begin to enroll on-line for a digital ID. You will be required to provide some basic information on the digital ID enrollment form including your name, phone number, email address, company name, job title and your digital ID Approval Code. When you submit this form, the information is electronically sent to NRC's VeriSign digital certificates administrator for review and approval. Within minutes of submitting you should receive back from NRC an email acknowledging receipt of your enrollment request. If your enrollment is approved, then a second email will be sent to you with instructions for installing your digital ID certificate. Approval may take up to three business days.

If your enrollment is approved, you will receive an email that contains two things: first it contains a 10-digit VeriSign-issued Personal Identification Number (PIN). Second, it contains a web link to the VeriSign certificate digital ID pick up site. For security purposes you are required to pick up your digital ID certificate from the same computer where you enrolled for this certificate. When you pick up the certificate, it is downloaded and installed into your PC's web browser. This certificate can then be exported (copied) to a removable media for backup, and it can be imported into other computers. It is your responsibility to protect your certificate both physically and with a strong password. We recommend setting certificate security to "High", which then requires you to enter your certificate password each time you go to use it. If a certificate password is forgotten, it cannot be reset. A new certificate must be requested).

5. How to Request an NRC Approval Code

To request an NRC Approval Code, you must first determine which NRC program meets your needs. Each program area will want basic information from you including your name, email address, phone number, organization, role in the organization and reason for submitting documents to the NRC.

Criminal History Program participants should call (301) 415-6511 or send an email request to the NRC's Criminal History Program staff at: CrimHist@nrc.gov

Adjudicatory Proceedings Program participants should call (301) 415-1679 or call (301) 415-1966 or send an email request to the NRC's Office of the Secretary staff at: HearingDocket@nrc.gov

NRC General Form Program participants should call (301) 415-0439 or send an email request to the NRC's General Form Program staff at: GeneralForm@nrc.gov

ERDS participants should send an email request to the NRC's ERDS staff at: ERDS@nrc.gov

Fitness for Duty Reporting participants should call (301) 415-5949 or send an email request to the NRC's Fitness for Duty Reporting staff at: FitnessForDutyResource@nrc.gov

6. Digital ID Certificate Enrollment Steps

IMPORTANT: You must pick up your digital ID certificate from the same PC where you enrolled. This is a security precaution imposed by VeriSign. Therefore only enroll from a PC where you receive email for the email address to be associated with your certificate.

Prior to starting the Digital ID enrollment process, you must first have an NRC Approval Code since this is a required field in the electronic enrollment form. If you don't have an NRC Approval Code, follow the instructions within Section 5 of this document to get an approval code.

1. Open your Internet Explorer browser.
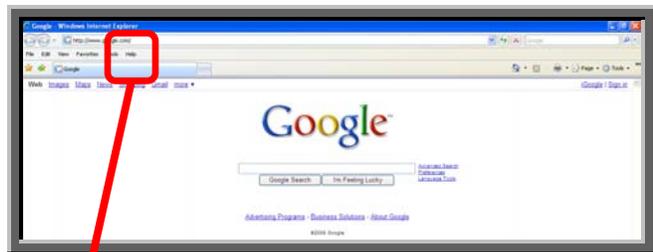
2. Determine if you have Internet Explorer 7.0 by selecting the [Help] tab. Scroll down and select: [About Internet Explorer]

♦ ♦

3. An "About Internet Explorer" dialogue box will appear, displaying the version.

Select the [OK] button to close the dialogue box.

4. For Internet Explorer 7.0 users, the following steps must be conducted prior to successfully completing the enrollment process if security is set to "High" or "Medium High". You must reduce your PC's Internet Explorer security to "Medium" for the enrollment process. After installing the certificate to your computer, you may reset the security to "High" again.
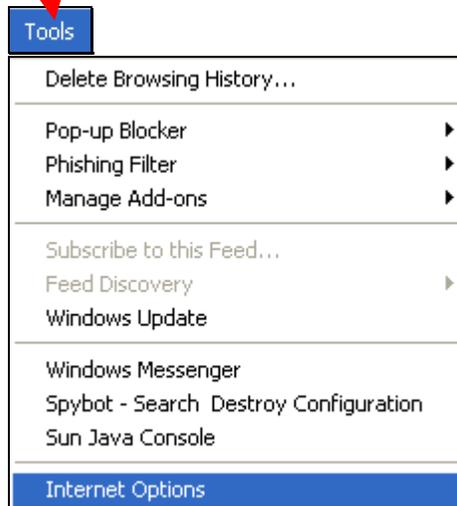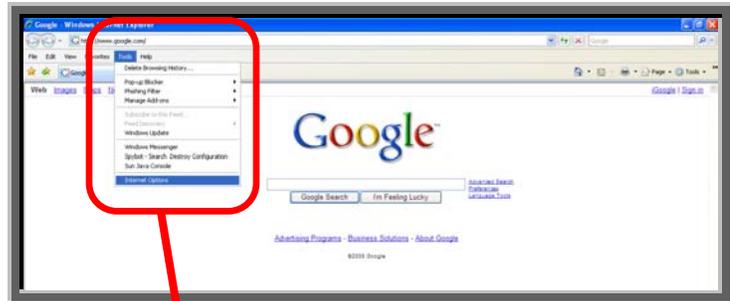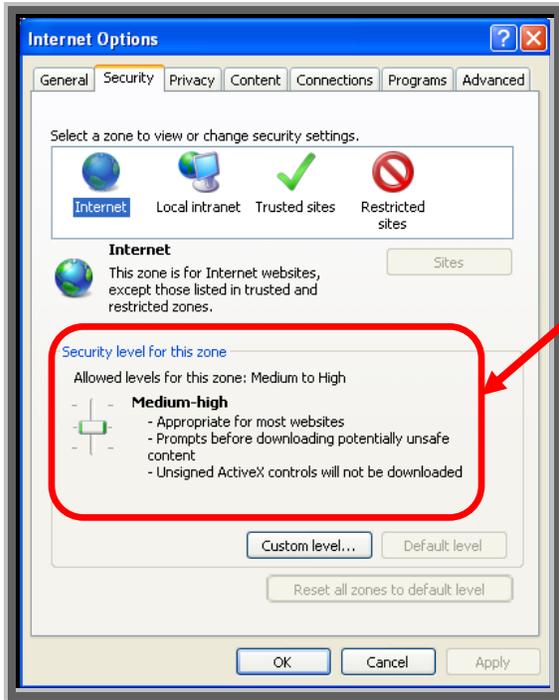

5. Click on the [Tools] tab. Then scroll down and select:
    [Internet Options]

◆ ◆
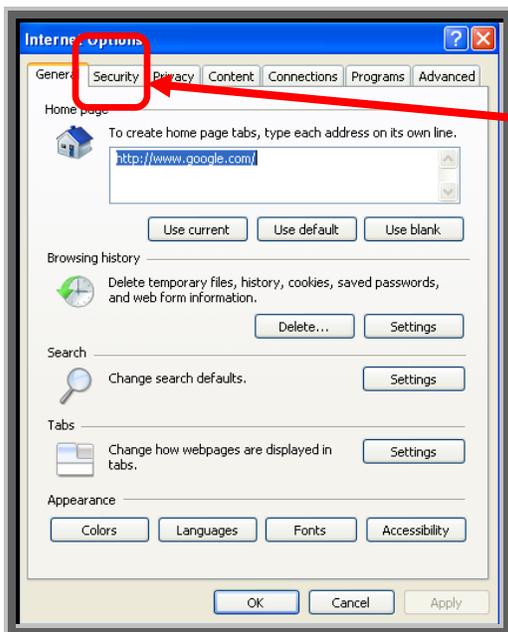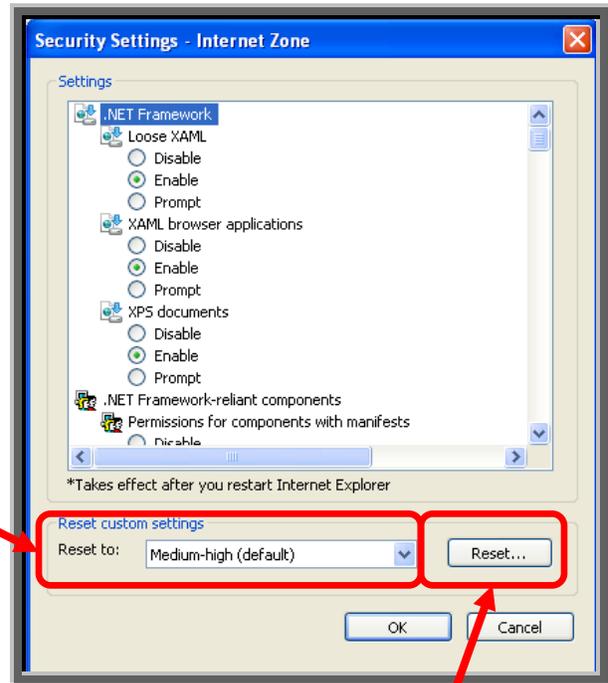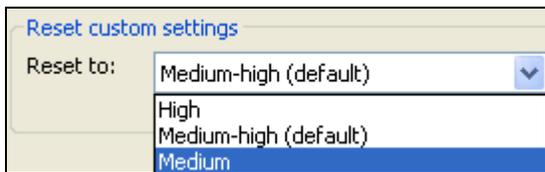

6. Select the [Security] tab.

7. Below *Security level for this zone*, the security level is displayed.
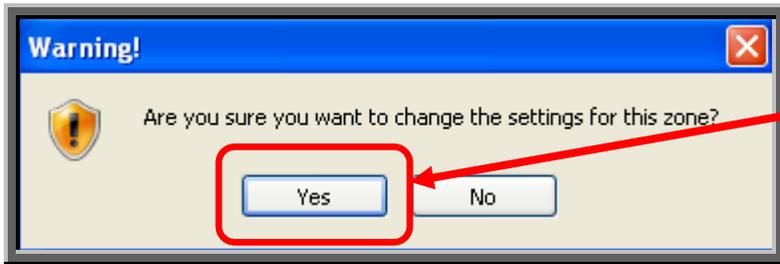

Is the security level set at "Medium"?

Yes   Continue with the instructions on Page 9, Step #12.

No   Click on the [Custom level...] button, then continue with the Step #8 below.

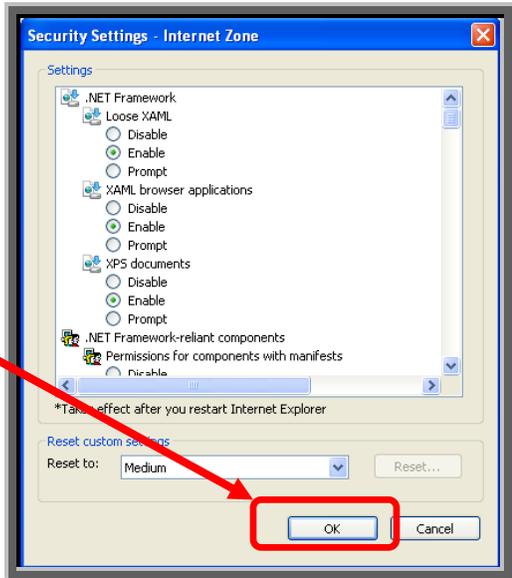8. Below *Reset custom settings*, select the drop-down menu within the **Reset to:** field. Scroll down and select: [Medium]
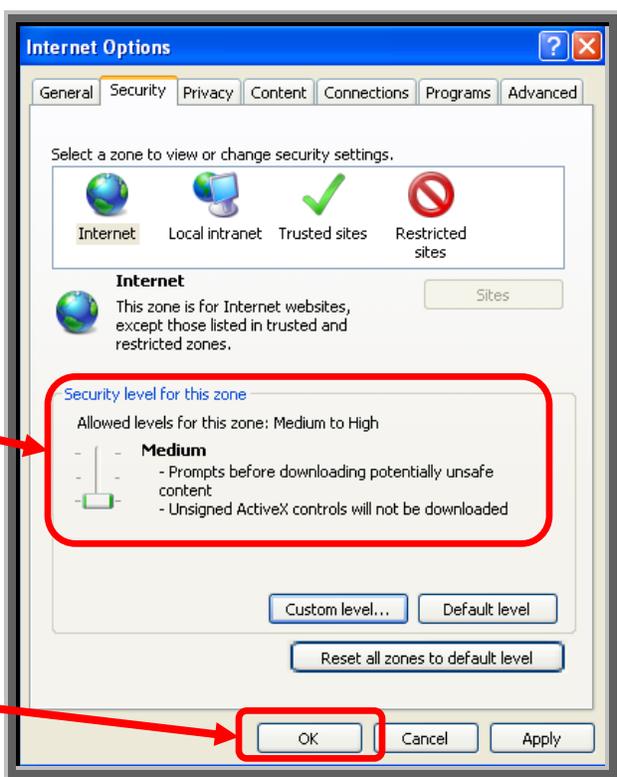

9. Select the [Reset...] button.

Warning!

Are you sure you want to change the settings for this zone?

[Yes]   [No]

10. A Warning! dialogue box will appear. Select the [Yes] button to change the settings.

♦ ♦ ♦ ♦ ♦ ♦ ♦ ♦ ♦ ♦ ♦ ♦ ♦ ♦ ♦ ♦ ♦ ♦ ♦ ♦

Security Settings - Internet Zone

Settings

.NET Framework
  Loose XAML
    ○ Disable
    ● Enable
    ○ Prompt
  XAML browser applications
    ○ Disable
    ● Enable
    ○ Prompt
  XPS documents
    ○ Disable
    ● Enable
    ○ Prompt
.NET Framework-reliant components
  Permissions for components with manifests
    ○ Disable

*Takes effect after you restart Internet Explorer

Reset custom settings

Reset to: Medium   [Reset...]

[OK]   [Cancel]

11. Select the [OK] button.

♦ ♦ ♦ ♦ ♦ ♦ ♦ ♦ ♦ ♦ ♦ ♦ ♦ ♦ ♦ ♦ ♦ ♦ ♦ ♦

Internet Options

General | Security | Privacy | Content | Connections | Programs | Advanced

Select a zone to view or change security settings.

Internet | Local intranet | Trusted sites | Restricted sites

Internet
This zone is for Internet websites, except those listed in trusted and restricted zones.

[Sites]

Security level for this zone

Allowed levels for this zone: Medium to High

Medium
  - Prompts before downloading potentially unsafe content
  - Unsigned ActiveX controls will not be downloaded

[Custom level...]   [Default level]

[Reset all zones to default level]

[OK]   [Cancel]   [Apply]

12. Below *Security level for this zone*, the security level displayed is **Medium**.

13. Select the [OK] button.

The steps to enroll for an NRC-issued digital ID certificate are:

14. Navigate to the NRC's public website: www.nrc.gov .

15. Move your mouse cursor over the **Business with NRC** button located on the left side of the screen. A drop-down menu will appear. Select **Electronic Submittals** .

16. From the "Electronic Submittals" website (http://www.nrc.gov/site-help/e-submittals.html), scroll down to the "**Submittal Instructions**" section and select the NRC's Digital ID Center.

◆ ◆

17. Select **ENROLL** .
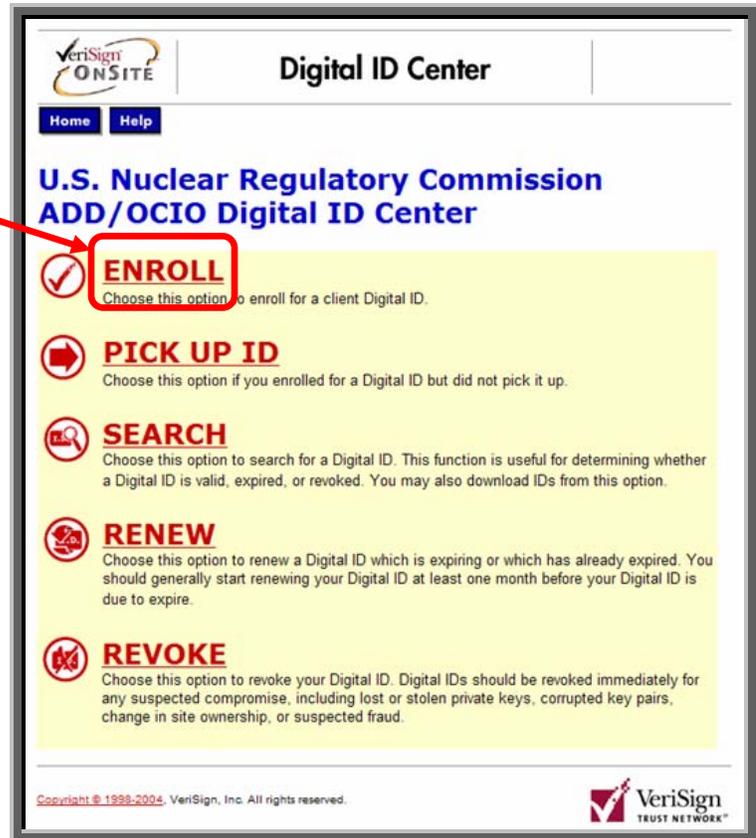
18. The Enrollment Form will be displayed.

VeriSign OnSite | **Enrollment**

Help with this Page

Complete Enrollment Form

Enter your Digital ID information

Fill in all required fields. Fields marked with an asterisk **(*)** are included with your Digital ID and are viewable in the certificate's details.

First Name: * (required) Nickname or middle initial allowed (Example: Jack B.)	
Last Name: * (required) (example -- Doe)	
Your E-mail Address: * (required) (example -- jbdoe@verisign.com)	
Title: * (Example: Programmer)	
NRC Certificate Approval Code: (required)	
Organization Name: * (required)	
Phone Number: * (required)	

Helpful tips for filling out the Enrollment Form:
- Include your middle initial after your first name as in "John D".
- The email address you enter will be stored on your digital ID certificate and has multiple uses including:
  ① It is used to send your certificate to you
  ② It must match the email address stored in NRC access list(s) in order for you to be able to submit documents other than through the General Form
  ③ It is used to send your annual renew reminder messages.
- The challenge phrase is needed for you to revoke your certificate if, for example, you change jobs and no longer need a certificate. It may also be needed a year from now in order to renew your digital ID certificate.
- The challenge phrase rules are:
  ① 1 to 32 characters long
  ② Only letters, numbers and/or spaces
  ③ Case and space sensitive (avoid trailing blanks)
  ④ Spaces and numbers are not required
  ⑤ Punctuation is not allowed
- The "**Optional: Enter Comments**" can be ignored since this is not used by the NRC.

---

19. Complete the online enrollment form, populating all required fields.

Note: When entering your E-mail Address, ensure it is correct before submitting your request.

Challenge Phrase
The Challenge Phrase is a unique phrase that protects you against unauthorized action on your Digital ID. Do not share it with anyone. *Do not lose it*. You will need it when you want to revoke or renew your Digital ID.
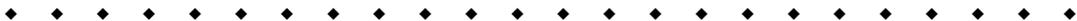
Enter Challenge Phrase: (required) Do not use any punctuation.	

Optional: Enter Comments
In some cases, your administrator will instruct you to enter *Shared Secret* information (known only to you and the administrator) in this field. The administrator uses this shared secret to verify that it really is *you* submitting the application. This comment will not be included in your Digital ID.

20. After verifying the fields were populated correctly, scroll to the bottom of the screen and click on the

Submit

button to submit your application.

If all the information above is correct, click **Submit** to continue.

Submit   **Cancel**

VeriSign
TRUST NETWORK℠

Challenge Phrase
The Challenge Phrase is a unique phrase that protects you against unauthorized action on your Digital ID. Do not share it with anyone. *Do not lose it*. You will need it when you want to revoke or renew your Digital ID.

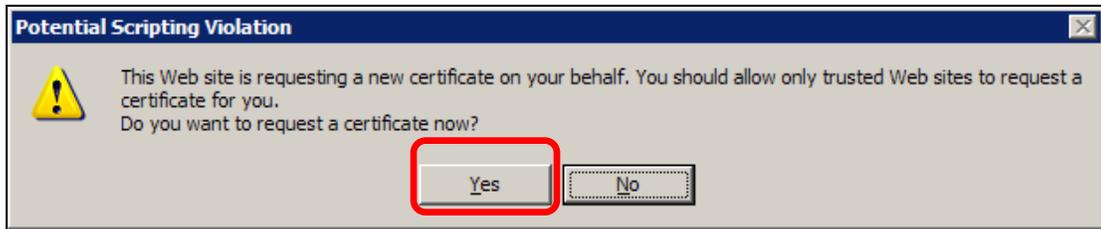**Enter Challenge Pl**
Do not use any punctu

Windows Internet Explorer

Confirm your e-mail address:
slm7@nrc.gov

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

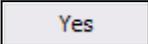If the e-mail address is not correct, you will not be able to use your Digital ID.

OK   Cancel

Optional: Enter Co
In some cases, your ad
to you and the administ
really is *you* submitting the application. This comment will not be included in your Digital ID.

If all the information above is correct, click **Submit** to continue.

Submit   **Cancel**

VeriSign
TRUST NETWORK℠

21. **Did you receive the *Confirm your e-mail address:* dialogue box?**

Yes Click on the

OK

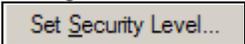button, then continue with the Step #22 instructions on the next page.

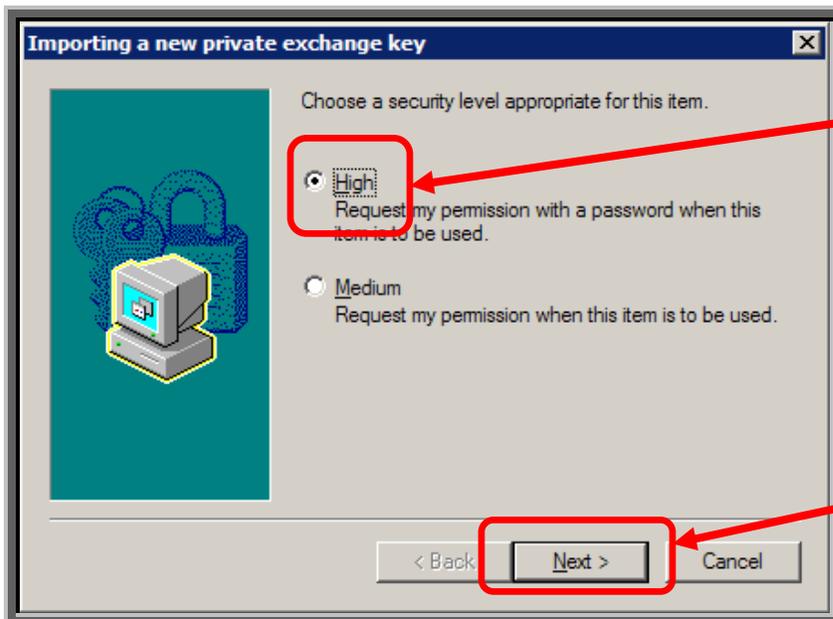**No** Continue with the Step #22 instructions on the next page.

22. Did you receive the *Potential Scripting Violation* dialogue box?

Potential Scripting Violation

⚠ This Web site is requesting a new certificate on your behalf. You should allow only trusted Web sites to request a certificate for you.
Do you want to request a certificate now?

[Yes]   [No]

Yes   Click on the [Yes] button, then continue with the Step #23 instructions below.
No   Continue with the Step #23 instructions below.

♦ ♦

23. At the *Creating a new RSA exchange key* dialogue box, click on the [Set Security Level...] button.

Creating a new RSA exchange key

An application is creating a Protected item.

CryptoAPI Private Key

Security level set to Medium   [Set Security Level...]

[OK]   [Cancel]   [Details...]

♦ ♦

Importing a new private exchange key

Choose a security level appropriate for this item.

⦿ 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.
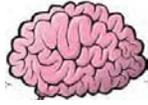
[< Back]   [Next >]   [Cancel]

24. Click on the radio button for High (⦿ High). This will activate the password protection for your digital ID certificate.
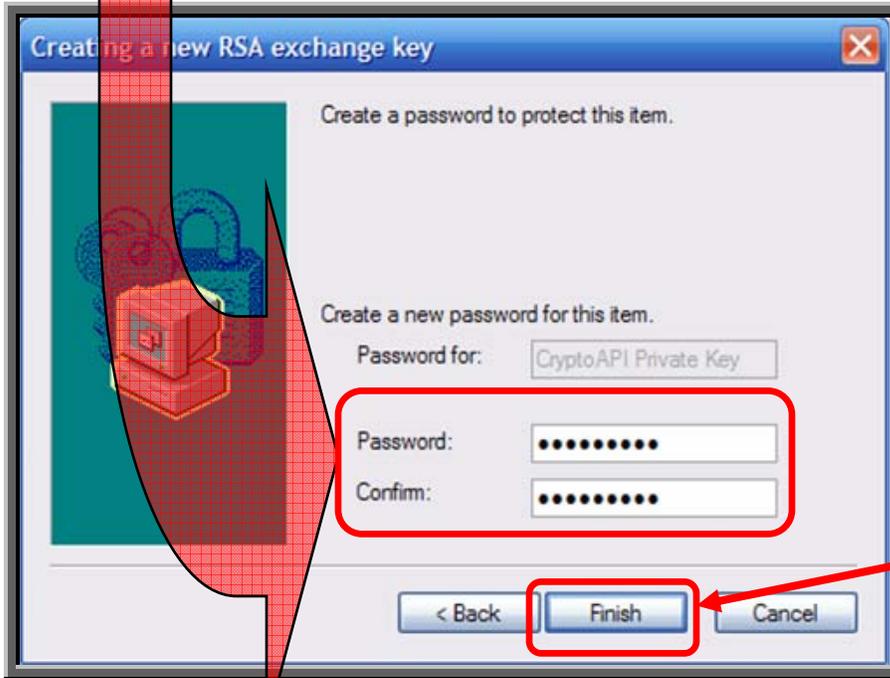
25 Click on the [Next >] button to continue.

26. Create and enter the **new password twice**.

<table>
<tr><td><u>Note</u>:</td><td>Commit to memory this password as it will be necessary to enter this password each time you use the certificate. If a certificate password is forgotten, it cannot be reset. A new certificate must be requested.</td></tr>
</table>

Creating a new RSA exchange key

Create a password to protect this item.

Create a new password for this item.

Password for: CryptoAPI Private Key

Password: •••••••••

Confirm: •••••••••

< Back   Finish   Cancel

27. After entering the password twice, click on the Finish button.

28. The Security level is now set to High. Click on the OK button.

Importing a new private exchange key

An application is creating a Protected item.

CryptoAPI Private Key

Security level set to High   Set Security Level...

OK   Cancel   Details...

You have now successfully requested your digital ID certificate. A notification will appear to **Look in Your E-mail**.
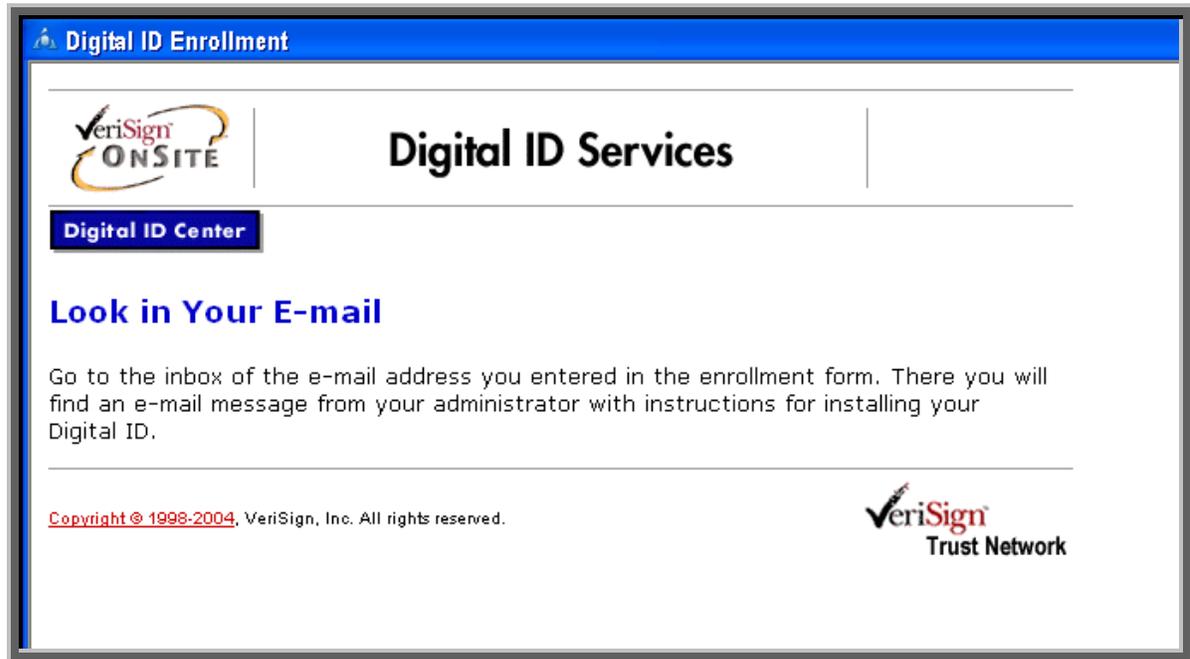
Within minutes you should receive an email acknowledging receipt of your enrollment request.

Within several hours (Eastern Standard Time business hours) your request should be reviewed and approved or disapproved. You should then receive a second email. The approval email's subject is: "Your Digital ID is ready".

Follow the instructions in this document for installing a digital ID certificate (see Section 7, Digital ID Certificate Installation Steps).

If you have not received an approval or rejection email within two business days, send an email to DigitalIDHelp@nrc.gov or call (301) 415-0439.

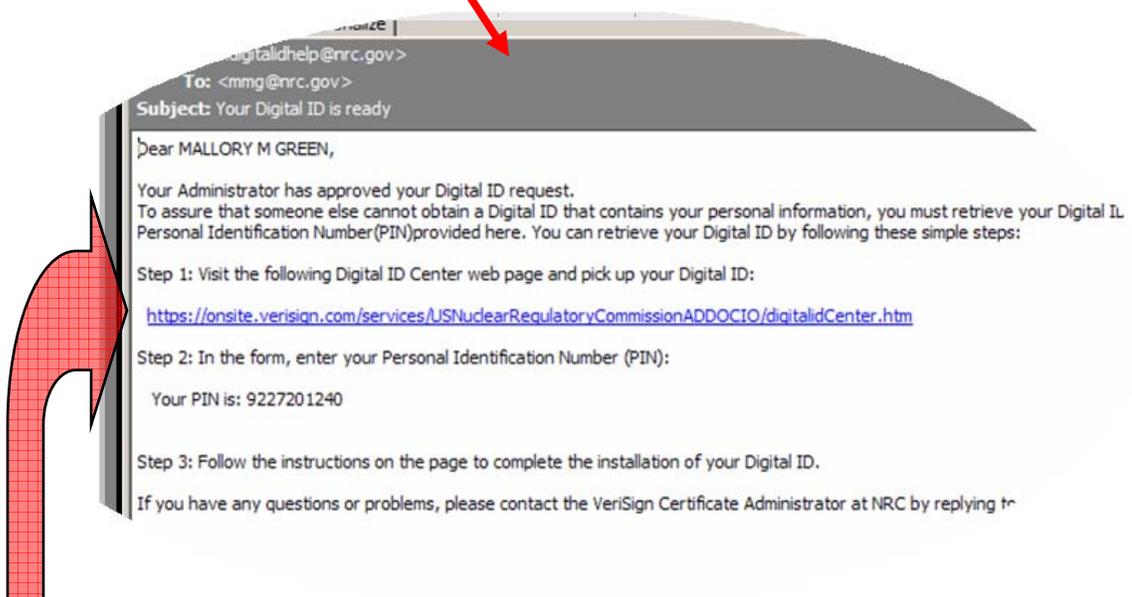# 7. Digital ID Certificate Installation Steps

You will receive a "Your Digital ID is ready" email, if your digital ID certificate request is approved. This email will contain both a VeriSign provided Personal ID Number (PIN) and a link to NRC's Digital ID Center.

The steps to pick up and install your digital ID certificate are:

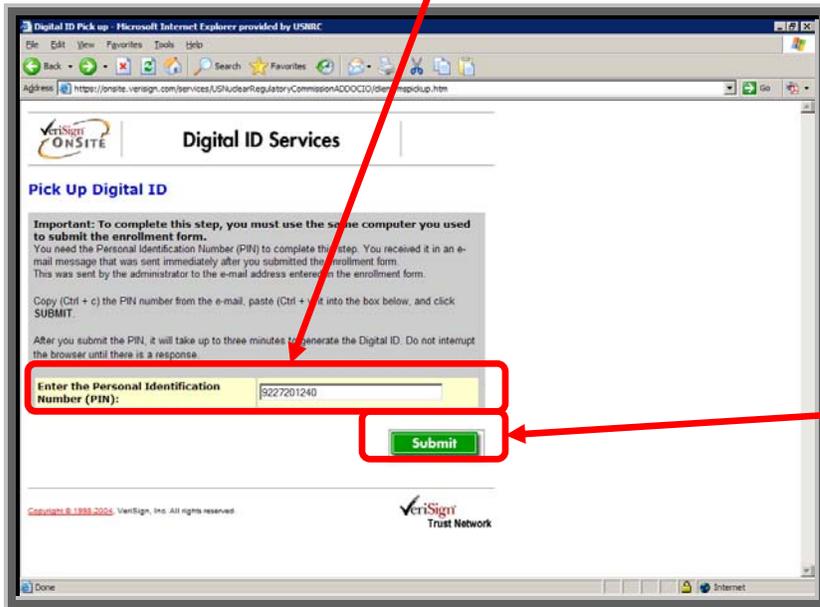1. Open the "**Your Digital ID is ready**" email message.
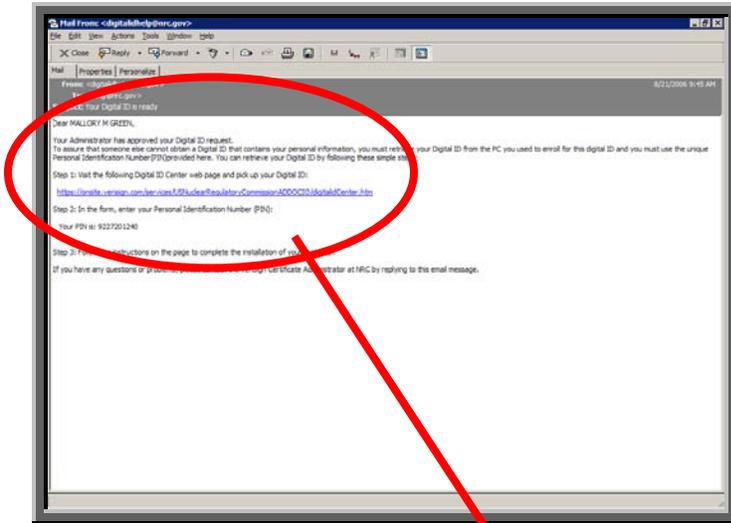
2. Copy the PIN (provided in Step 2 of the email message). An easy copying method is to highlight the PIN then right-mouse click and select the "**Copy**" option.

To: <mmg@nrc.gov>

Subject: Your Digital ID is ready

Dear MALLORY M GREEN,

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
Personal Identification Number(PIN)provided here. You can retrieve your Digital ID by following these simple steps:

Step 1: Visit the following Digital ID Center web page and pick up your Digital ID:

https://onsite.verisign.com/services/USNuclearRegulatoryCommissionADDOCIO/digitalidCenter.htm

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

   Your PIN is: 9227201240

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 the VeriSign Certificate Administrator at NRC by replying to

3. Next, click on the link (provided in Step 1 of the e-mail message), which takes you to NRC's Digital ID Center's "**PICK UP ID**" web page.

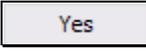4. Click within the **Enter the Personal Identification Number (PIN)** field and paste the PIN into the field (an easy way to do this is by pressing the `Ctrl` key on the keyboard and the `V` key).

5. Click on the

button.

◆ ◆

---

6. Did you receive a *Potential Scripting Violation* dialogue box (see screen print below)?

Yes Click on the `Yes` button, then continue with the instructions at the top of the next page.

No Continue with the instructions at the top of the next page.
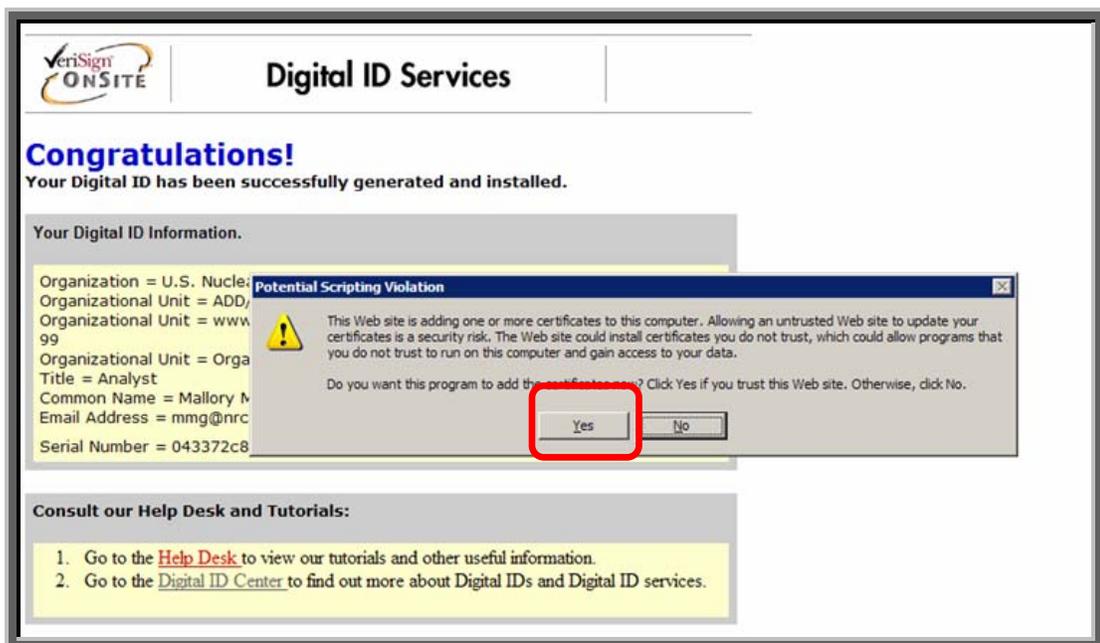
You will receive a **Congratulations!** screen telling you that your digital ID certificate have been successfully generated and installed.
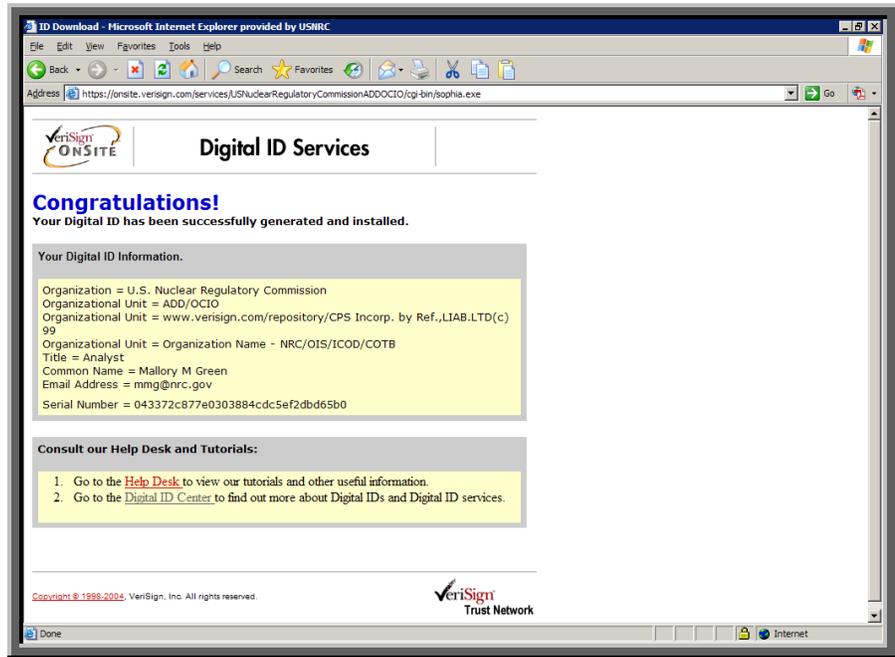
8. Digital ID Certificate Viewing Steps

Your VeriSign digital ID certificate is installed into your browser. The following steps on your PC may be somewhat different depending upon your browser, browser version, browser setting, operating system and operating system settings.

To view your certificate in the Internet Explorer browser Version 6.0, complete the following steps:
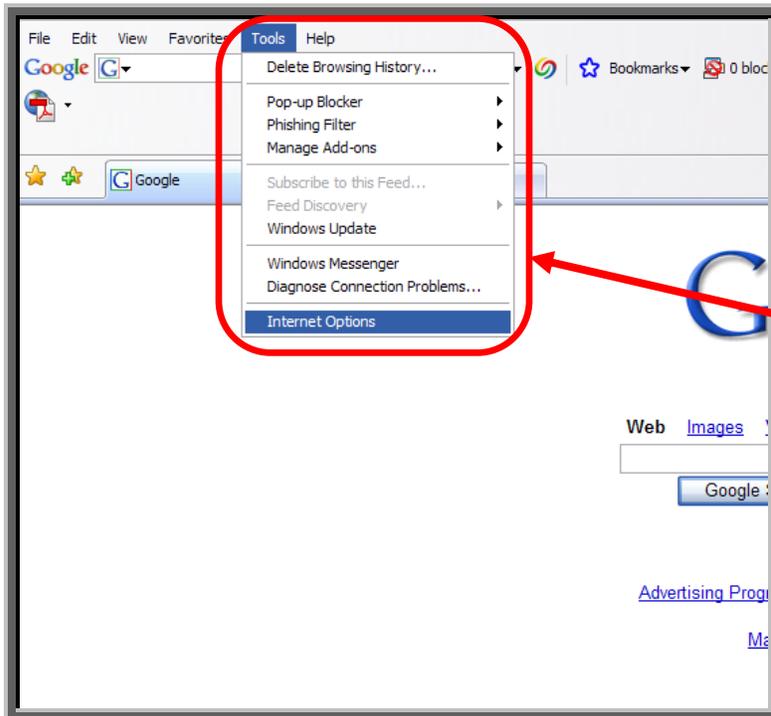
1. Open Internet Explore and click on the **Tools** tab. From the drop-down menu select **Internet Options**.

2. Select the Content tab in the Internet Options window.
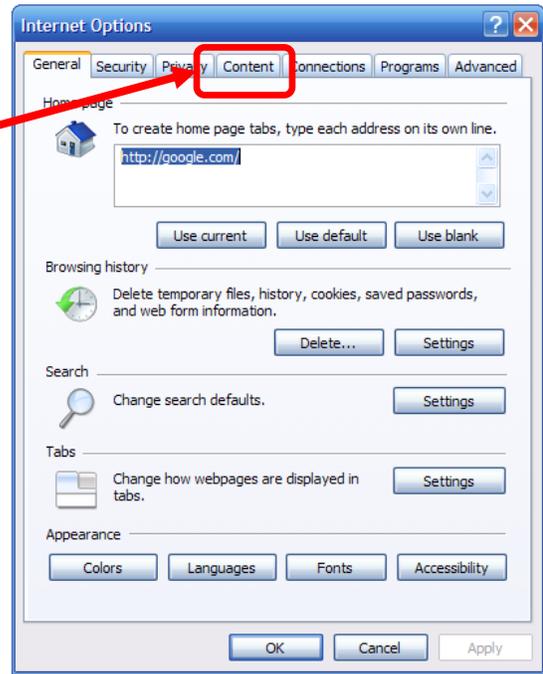
Note: Under some restricted computer access and security settings users may not have all the above Internet Options tabs and may be prevented from seeing, exporting or deleting their digital ID certificates via their computer browser.
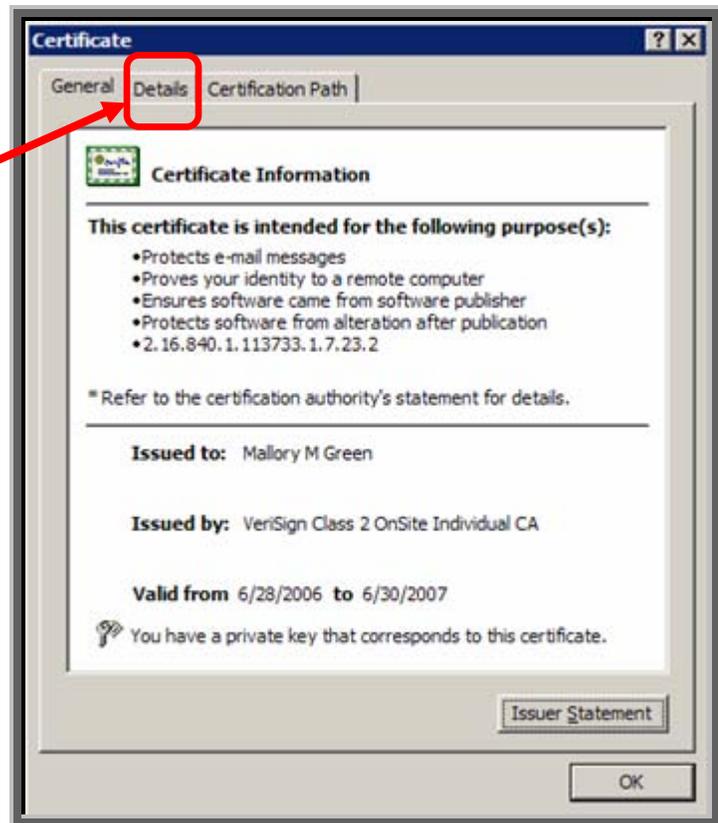
◆ ◆
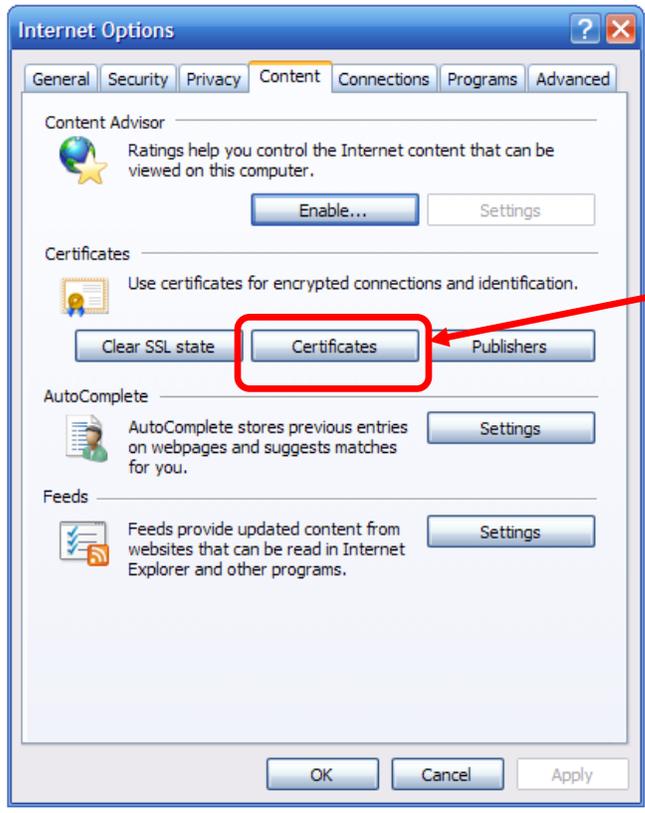
3. Click on the Certificates button.

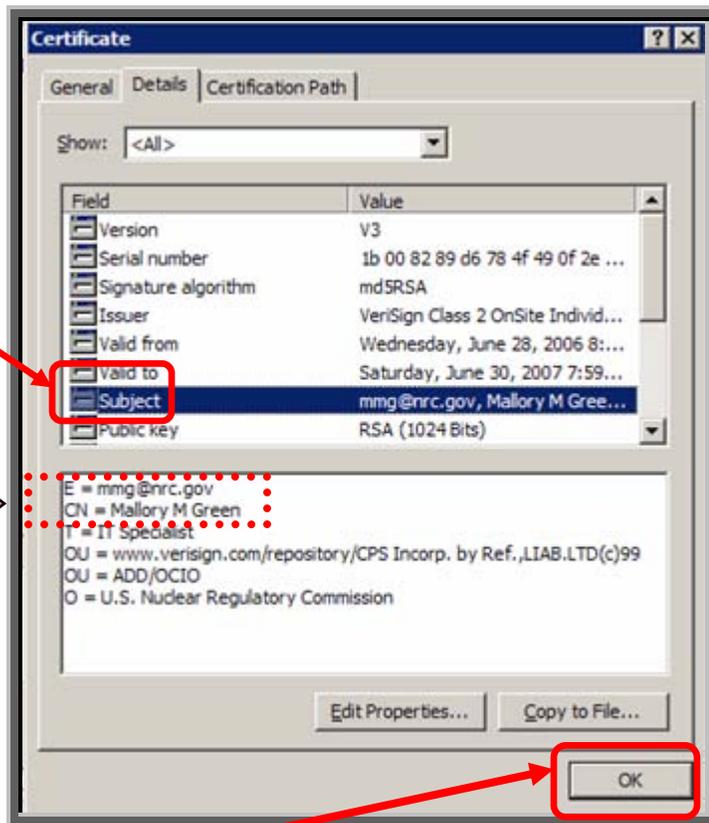4. Choose a certificate to view by clicking on the desired certificate.

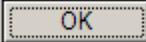5. Click on the **View** button to see information about the selected certificate.
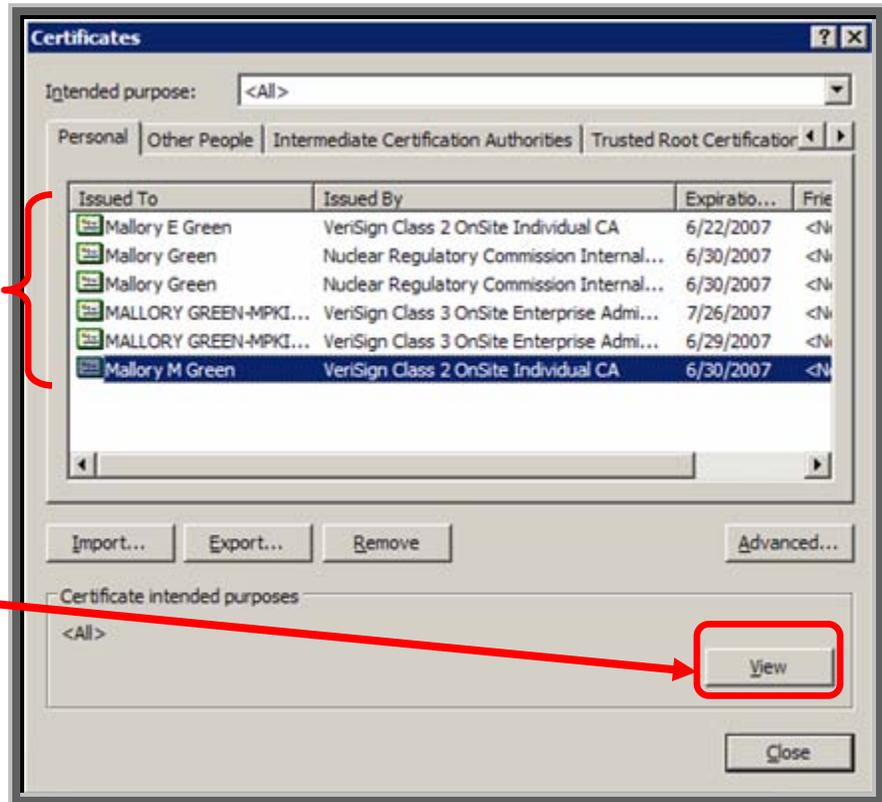
6. Click on the **Details** tab.

7. Click on the **Subject** field to see your data.

Notice that your email address is saved after E = and your name is saved after CN = in the certificates "Subject" field.
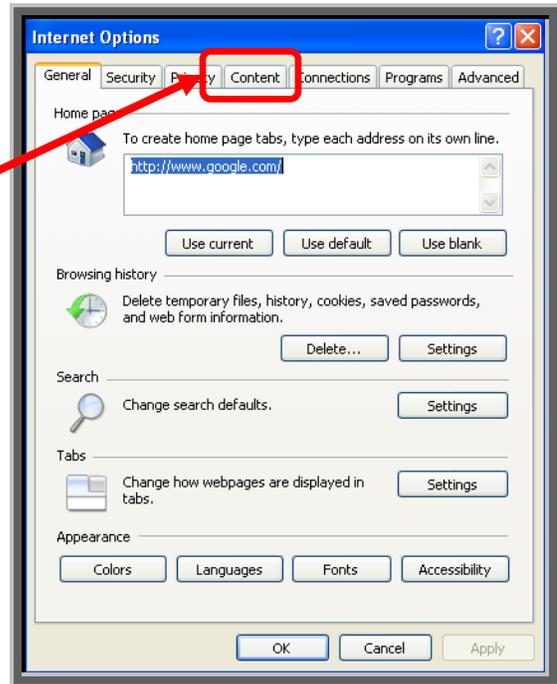
Certificate

General | Details | Certification Path

Show: `<All>`

Field	Value
Version	V3
Serial number	1b 00 82 89 d6 78 4f 49 0f 2e ...
Signature algorithm	md5RSA
Issuer	VeriSign Class 2 OnSite Individ...
Valid from	Wednesday, June 28, 2006 8:...
Valid to	Saturday, June 30, 2007 7:59...
Subject	mmg@nrc.gov, Mallory M Gree...
Public key	RSA (1024 Bits)

E = mmg@nrc.gov
CN = Mallory M Green
T = IT Specialist
OU = www.verisign.com/repository/CPS Incorp. by Ref.,LIAB.LTD(c)99
OU = ADD/OCIO
O = U.S. Nuclear Regulatory Commission

Edit Properties...   Copy to File...

OK

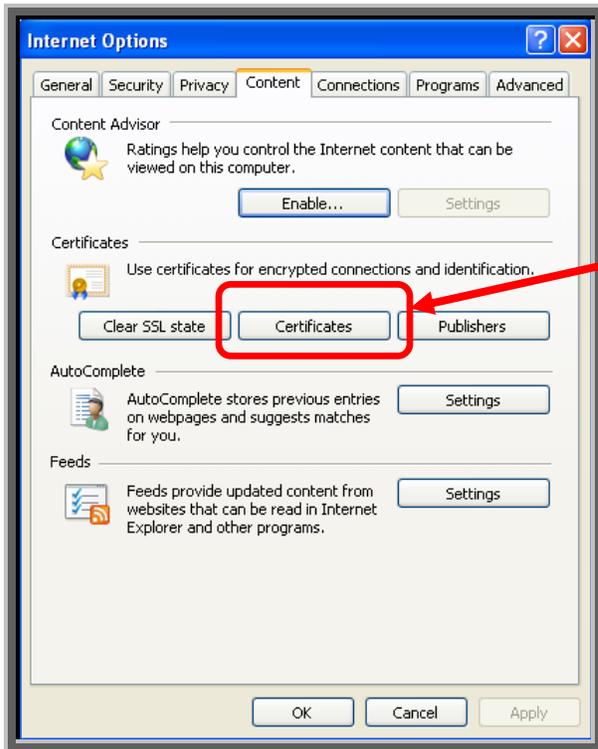8. Click on the **OK** button.

9. Digital ID Certificate Export

1. The certificate can be exported from one computer and imported onto another computer. Exporting does not remove the certificate, it simply copies the certificate to a file path location you choose (such as a removable media). To export the certificate, open your Internet Explore browser.

2. Click on the **Tools** menu option.
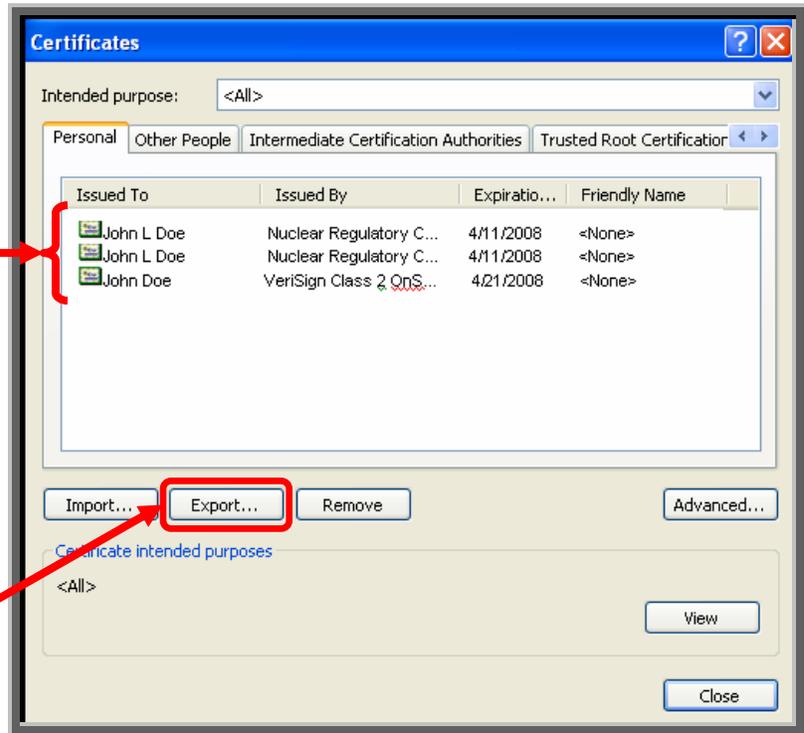
3. From the drop-down list, select **Internet Options**.
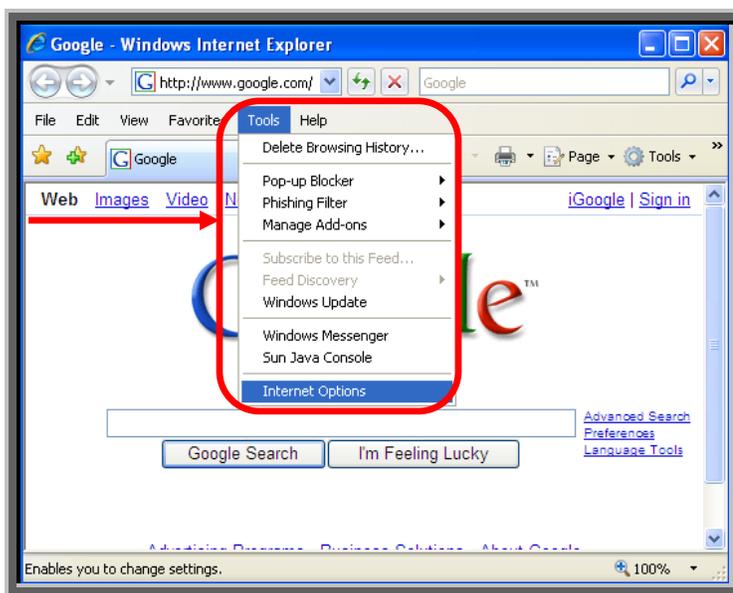
4.   Click on the `Content` tab.

♦ ♦

5.   Click on the `Certificates` button.

6. The Export button may not be activated. If this occurs, you must click on the certificate that is going to be exported (which is listed within the Personal tab). This will activate the Export button.

7. Click on the Export... button.

• •

8. From the Export Wizard dialogue box displayed, select the Next > button.

9. Ensure

⊙ Yes, export the private key

is selected.

10. Select the

Next > button.

Certificate Export Wizard

Export Private Key
You can choose to export the private key with the certificate.

Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

⊙ Yes, export the private key

○ No, do not export the private key

< Back   Next >   Cancel

◆ ◆

11. Select the following on the *Certificate Export File Format* screen;
  ⊙ **Personal Information Exchange**.
  ☑ **Include all certificates in the certificate path if possible**.
  ☑ **Enable strong protection (requires…)**.

Note: **DO NOT** proceed until you verify these three items are selected to ensure the export process is successful*!*

Certificate Export Wizard

Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

  ☐ Include all certificates in the certification path if possible

⊙ Personal Information Exchange - PKCS #12 (.PFX)

  ☑ Include all certificates in the certification path if possible

  ☑ Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)

☐ Delete the private key if the export is successful

12. Select the

Next > button.

< Back   Next >   Cancel
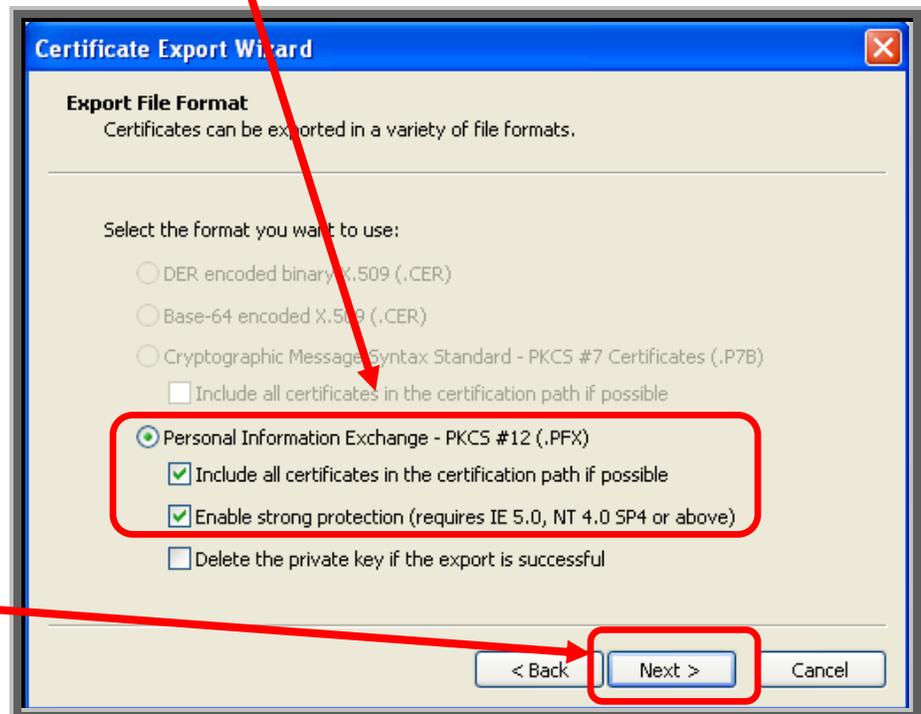
13. Type in an export/import password twice.

Note: This password is created during the export process and only used during the import process. It should not be confused with your digital ID certificate password set immediately after setting security to "High" for your certificate.
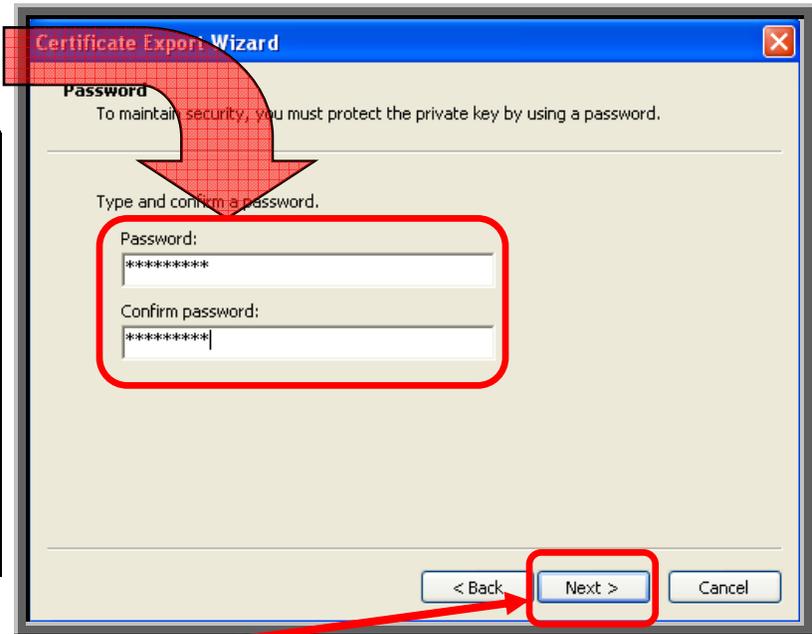

14. Select the [Next >] button.

◆ ◆

15. Select the [Browse...] button to navigate to the appropriate file path location of where the certificate is to be stored (such as a removable media).
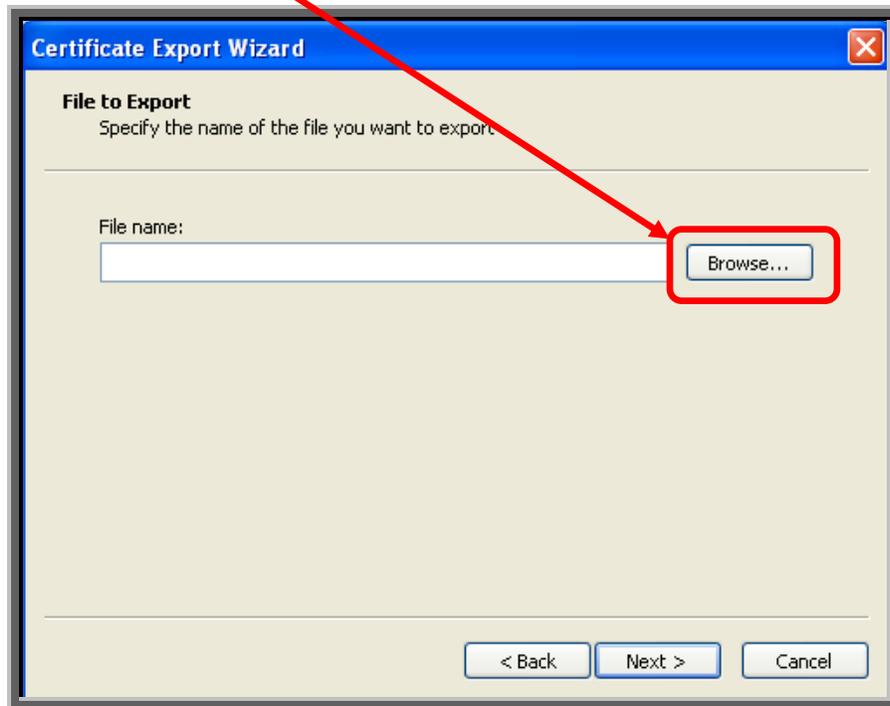
Note: If you know the file directory location of where the certificate is to be stored, you may simply type the file path into the **File name** field, then proceed to the instructions on Page 26, Step #18.

16. Type the certificate name within the **File name** field (the certificate file's extension is Personal Information Exchange (*.**pfx**)), then select the Save button.
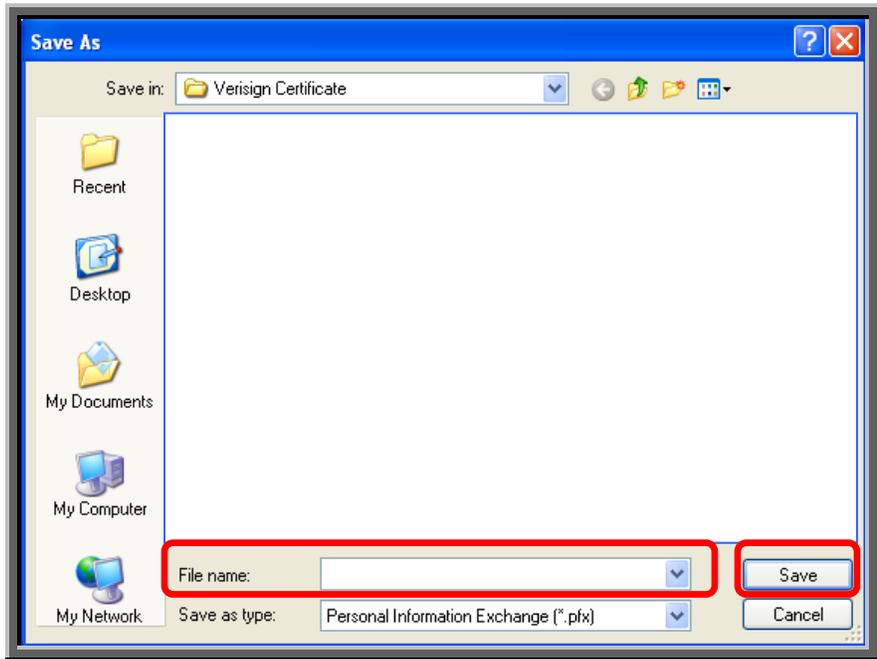
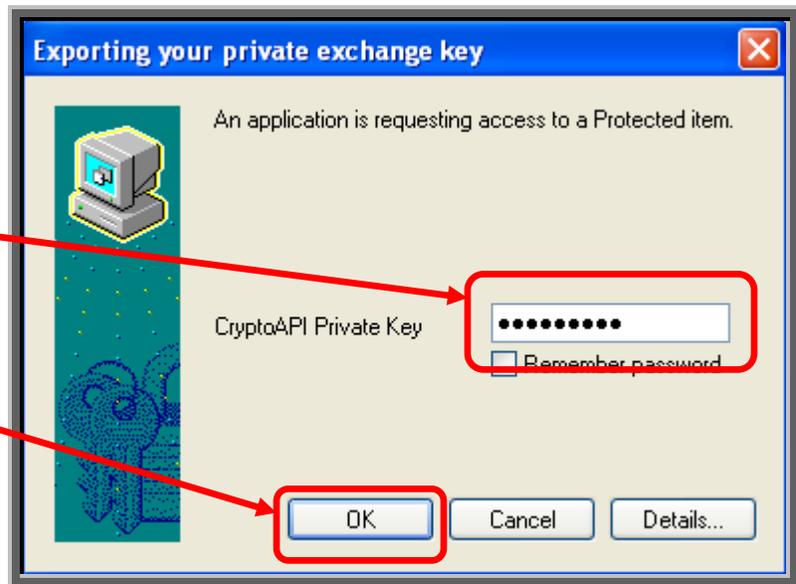17. The **File name** field will populate with the file path selection made.
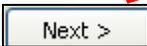
18. Select the Next > button.
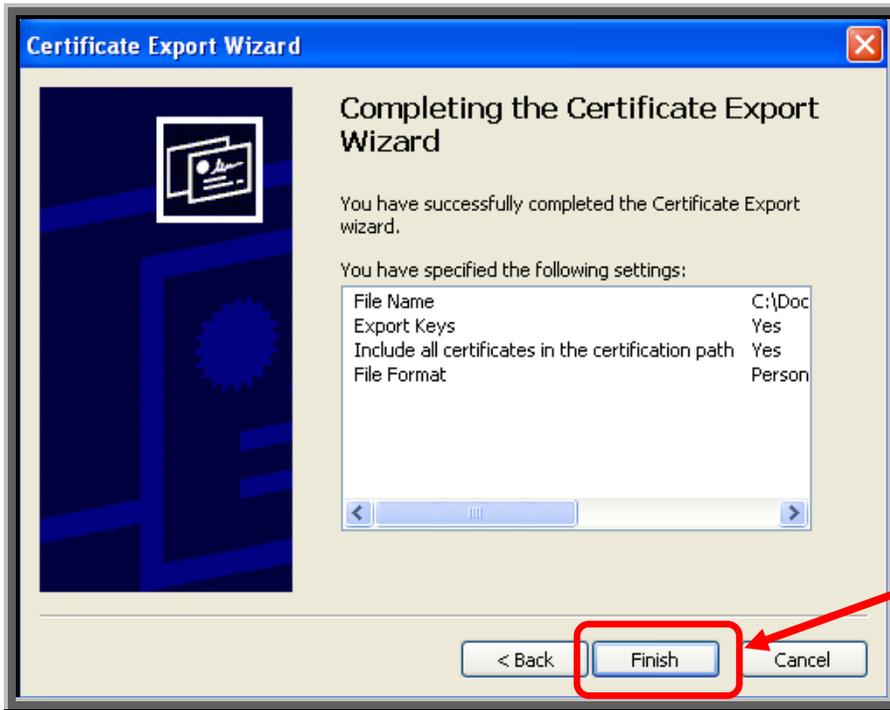
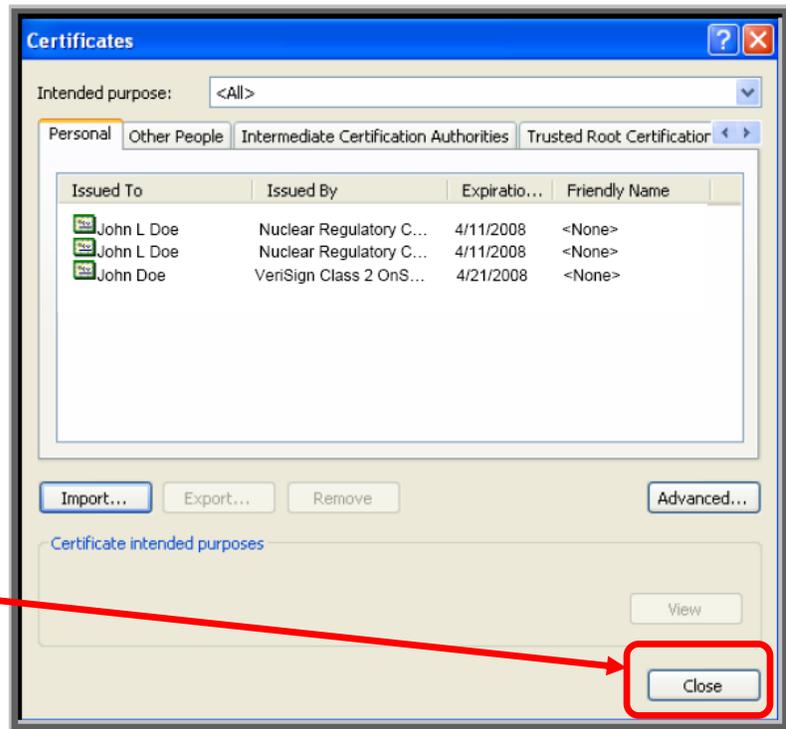19. At the *Completing the Certificate Export Wizard* dialogue box, select the Finish button.

20. Within the **CryptoAPI Private Key** field, enter the certificate password, then select the OK button.

21. A dialogue box will appear with the message that the export was successful. Select the OK button.

22. To complete the exporting process, select the Close button.
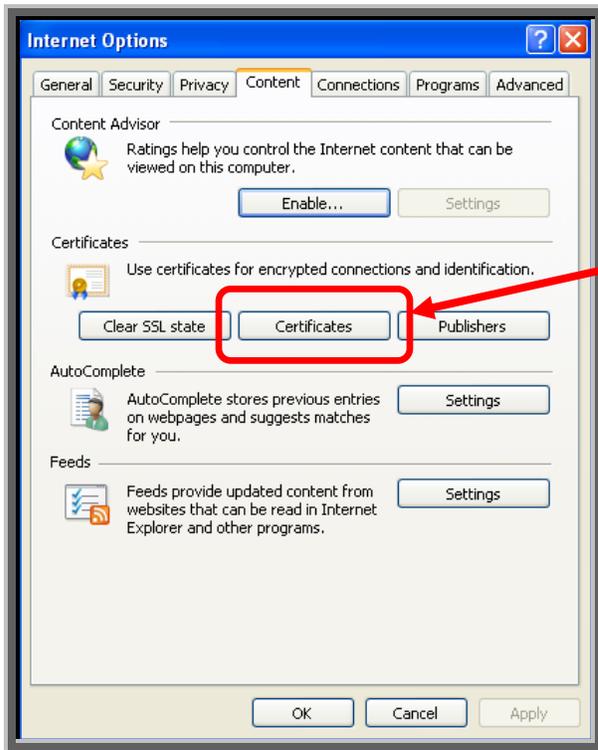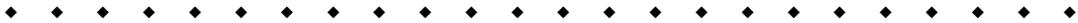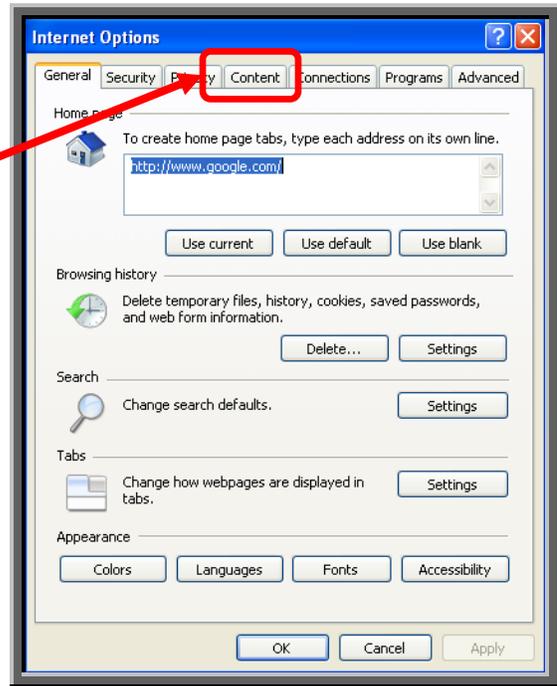
10. Digital ID Certificate Import

1. A certificate may be imported (copied) to a multiple number of computers. To import the certificate to a different computer (from where it was received), first open Internet Explore browser.

2. Select the Tools menu option.
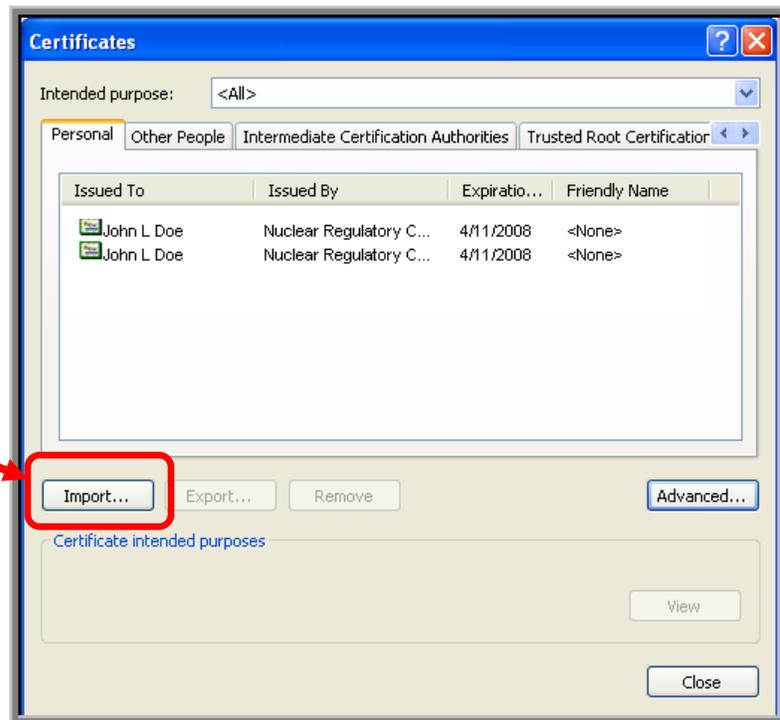
3. From the drop-down list, select Internet Options.
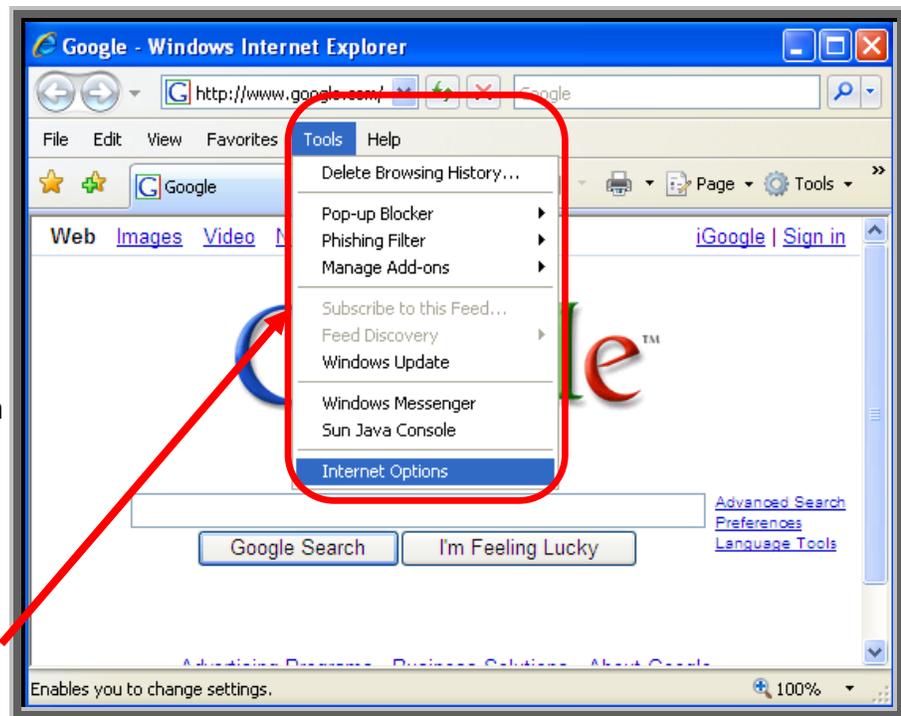
4.   Select the Content tab.

◆ ◆

5.   Select the Certificates button.

6. Select the **Import...** button.

7. A *Certificate Import Wizard* dialogue box will appear. Select the **Next >** button.

8. Enter the directory where the certificate is stored *or* select the Browse... button to navigate to the file path location of the certificate.

Note: If browsing to locate the certificate, within the **Files of Type** field (at the bottom of the *Open* dialogue box), using the drop-down menu, you must select "**Personal Information Exchange (*.pfx)**" in order to see the certificate file you are looking for.

---

9. After the **File name:** field is populated, select the Next > button.

♦   ♦

10. **Enter the export/import password** created during the certificate export process.
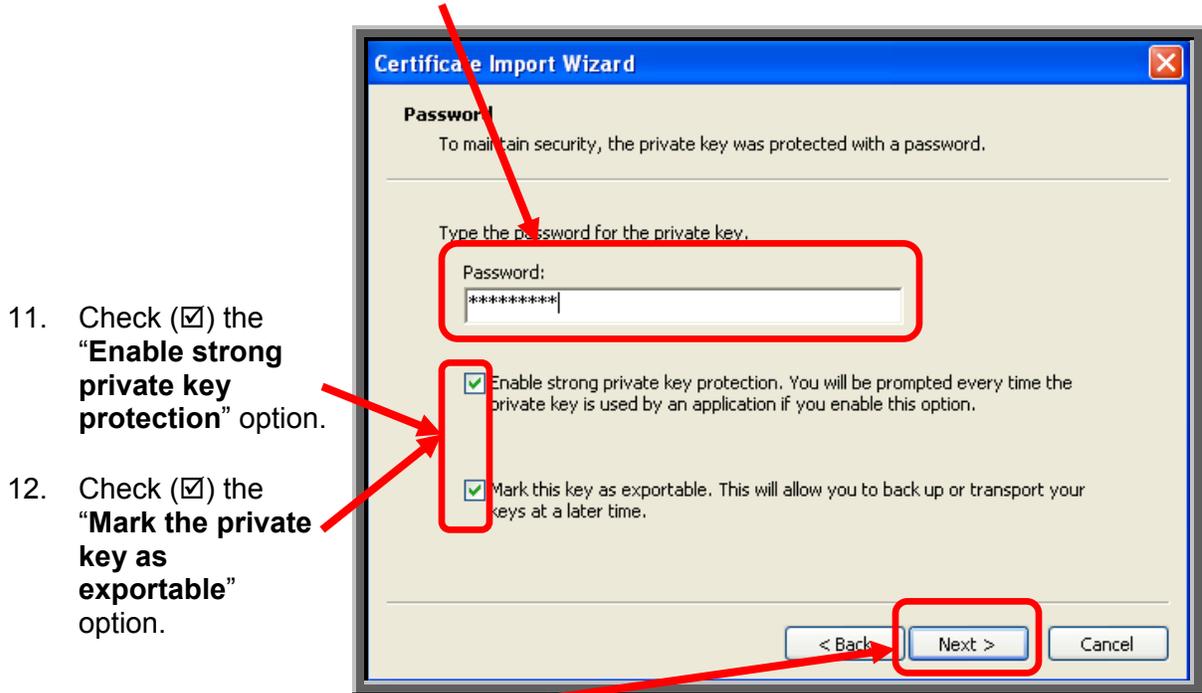
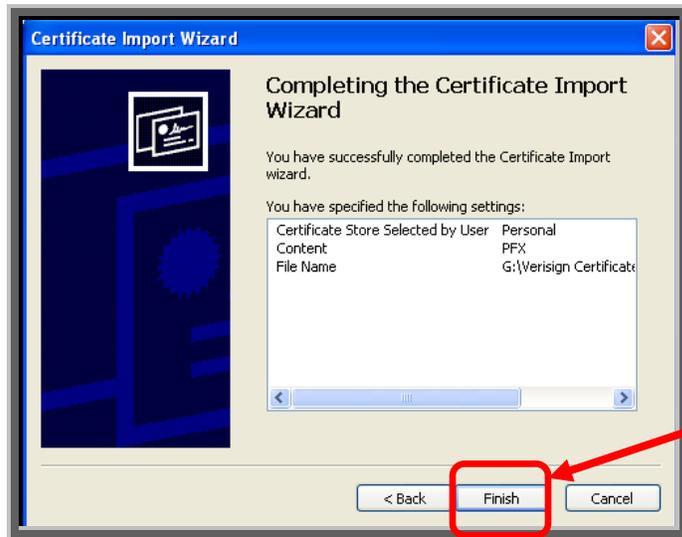11. Check (☑) the "**Enable strong private key protection**" option.

12. Check (☑) the "**Mark the private key as exportable**" option.

13. Select the Next > button.

14. Make sure the radio button is selected (⊙) for **"Place all certificates into the following store"** with the **Certificate Store:** field populated with **"Personal"**.
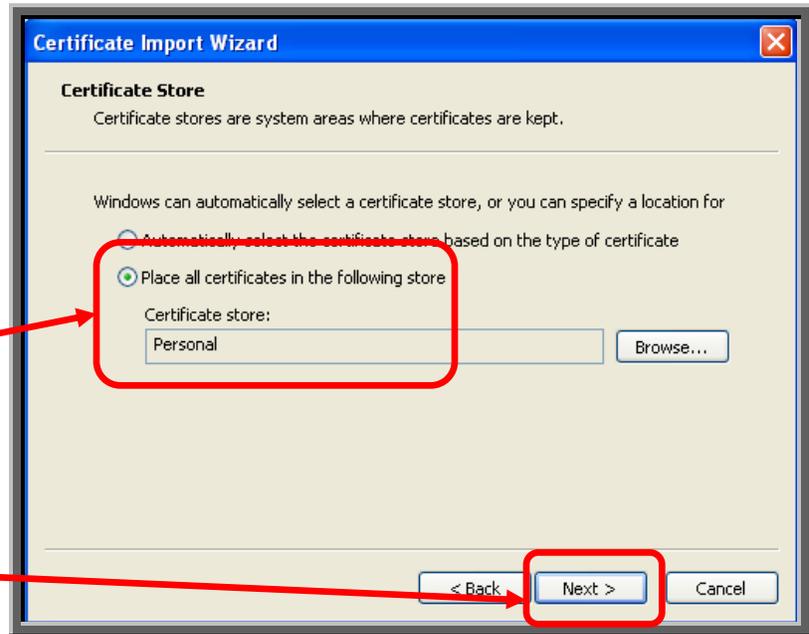
15. Select the [Next >] button.

♦ ♦

16. The *Completing the Certificate Import Wizard* dialogue box will appear. To exit, select the [Finish] button.

♦ ♦

17. The Security Level must be set to High. Select the [Set Security Level...] button.

18. Select the "**High**" (⊙ High) radio button. This will activate password protection for your digital ID certificate.

Importing a new private exchange key

Choose a security level appropriate for this item.

⊙ 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.

< Back   Next >   Cancel

19. Select the Next > button to continue.

◆ ◆

20. Enter the **new password twice**.

Note:	***Commit to memory*** this password as it will be necessary to periodically enter this password every time you use it, during the life of the certificate. If a certificate password is forgotten, it cannot be reset. A new certificate must be requested.

Creating a new RSA exchange key

Create a password to protect this item.

Create a new password for this item.
Password for: CryptoAPI Private Key

Password: ●●●●●●●●
Confirm: ●●●●●●●●

Finish   Cancel

21. Select the Finish button.

Importing a new private exchange key

An application is creating a Protected item.

CryptoAPI Private Key

Security level set to High   Set Security Level...

OK   Cancel   Details...

22. The Security level reveals it is now set to High.

23. Select the OK button.

Certificate Import Wizard

ⓘ The import was successful.

OK
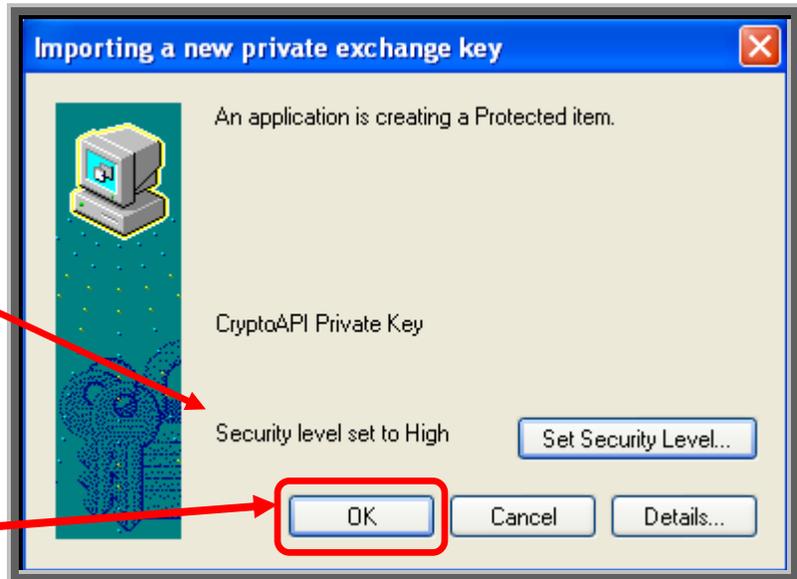
24. The message will appear that the import was successful. Select the OK button.

Certificates

Intended purpose: <All>

Personal | Other People | Intermediate Certification Authorities | Trusted Root Certification

Issued To	Issued By	Expiratio...	Friendly Name
John L Doe	Nuclear Regulatory C...	4/11/2008	<None>
John L Doe	Nuclear Regulatory C...	4/11/2008	<None>
John Doe	VeriSign Class 2 OnS...	4/21/2008	<None>

Import...   Export...   Remove   Advanced...

Certificate intended purposes

View

Close

25. The newly imported certificate will be displayed within the Personal tab.

26. To complete the importing process, select the Close button.
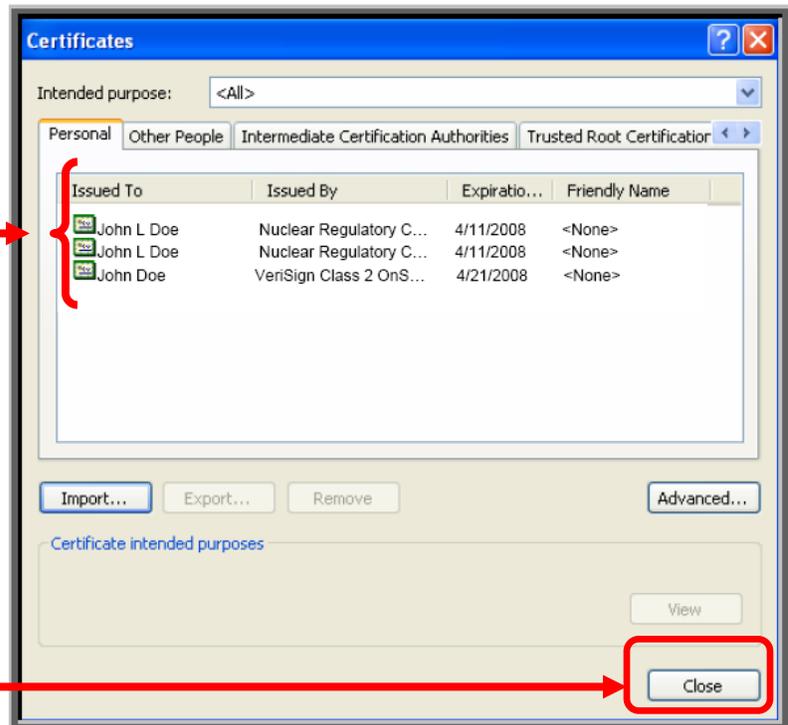
11. Digital ID Certificate Renewal

The NRC issues digital ID certificates from VeriSign with a one year term. You should receive an email message from the NRC first two weeks before and then again one week before your digital ID certificate is scheduled to expire. These email messages will include a link to a web address for you to request a replacement certificate. When you go to this link the software will verify that your certificate is on your PC and due to be renewed. You will be prompted to provide you digital ID certificates password. This is the password you established when you originally enrolled for you certificate and is required each time you use your certificate.

RENEW vs. ENROLL

You should enroll for a new certificate if:
- Your email address or name has changed since your enrollment last year.
- You have problems renewing your certificate. Sometimes the renewal process doesn't work correctly. Problems are likely to occur if your PC has been upgraded during the last year.

If the RENEW process doesn't work, then just ENROLL for a new certificate using your same name and email address. In this case, you may use the NRC Approval Code of: "RENEWAL". NRC's digital ID certificate administrator will review the records for your name and email address to confirm this is a renewal of a previously approved NRC digital ID certificate.

Enroll for a new digital ID certificate by going to NRC's Digital ID Center, https://onsite.verisign.com/services/USNuclearRegulatoryCommissionADDOCIO/digitalidCenter.htm and choosing the **ENROLL** option.
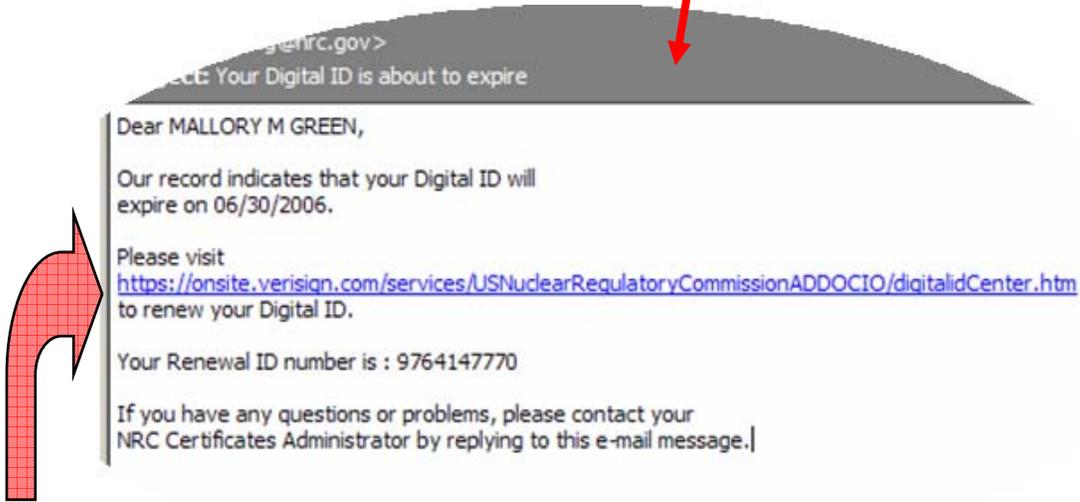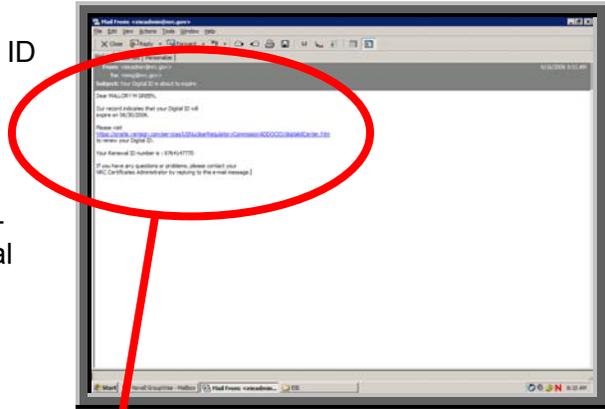
If you choose to ENROLL instead of RENEW because your name or email address has changed, you may also need to notify the associated NRC program area staff to update their access list(s) to reflect this name and/or email address change.

You should receive a "**Your Digital ID is about to expire**" email 2 weeks prior to and then 1 week prior to your certificate's expiration date.

> **Note:** You may also renew your digital ID certificate any time within one month of its expiration. To renew one month ahead of the expiration date, go to the NRC's Digital ID Center located at website: https://onsite.verisign.com/services/USNuclearRegulatoryCommissionADDOCIO/digitalidCenter.htm. Choose the **RENEW** option in the Digital ID Center, then follow the instructions beginning at step 3 below.

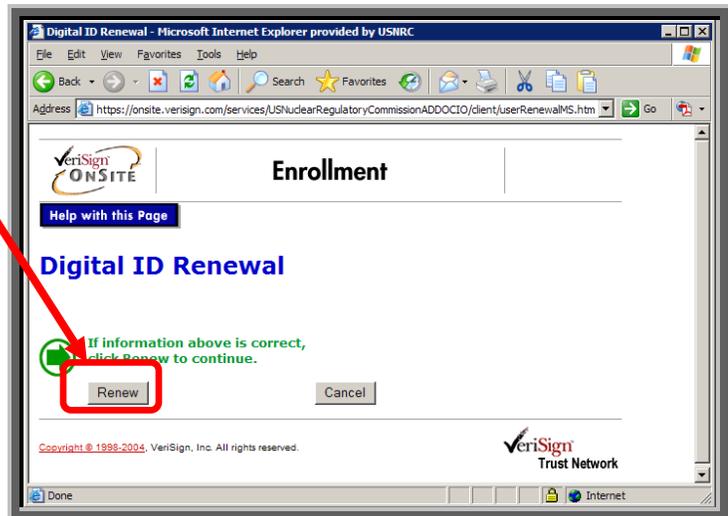Follow these instructions to renew your digital ID certificate:

1. Open your renewal email notice and copy the Renewal ID number (included in the e-mail message) by highlighting the Renewal ID number, then right-mouse click and choose "copy".

Dear MALLORY M GREEN,

Our record indicates that your Digital ID will expire on 06/30/2006.

Please visit
https://onsite.verisign.com/services/USNuclearRegulatoryCommissionADDOCIO/digitalidCenter.htm
to renew your Digital ID.

Your Renewal ID number is : 9764147770

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

2. Click on the provided link.

◆ ◆

3. Click on the [Renew] button in the **Enrollment** window.

Note: Do not worry when no information is displayed about your existing Digital ID. The reference to "**If information above is correct"** should really be asking you to confirm that you want to do a "Digital ID Renewal". Once you click on the [Renew] button, the next screen will give you information about the certificate to be renewed.

VeriSign Personal Trust Agent

Select Digital ID

Please select digital ID

VALID DATES
X / XX / 200X – X / XX / 200X
JOHN DOE

VeriSign   Renew   Cancel   Help

4. Click on the Renew button on a pop-up screen which contains your name and certificate dates
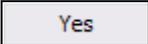
♦ ♦

5. Now you are asked to enter your certificate password. This is the same password you will enter every time you use this certificate since your certificate security is set to high. If your certificate security is not set to high, you will not see this pop-up window.

Signing data with your private exchange key

An application is requesting access to a Protected item.

CryptoAPI Private Key   ••••••••

☐ Remember password

OK   Cancel   Details...
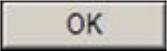
6. Click on the OK button.

7. Did you receive the *Potential Scripting Violation* dialogue box?

Potential Scripting Violation

⚠ This Web site is requesting a new certificate on your behalf. You should allow only trusted Web sites to request a certificate for you.
Do you want to request a certificate now?

[Yes]   [No]

Yes Click on the [Yes] button, then continue with the Step #8 instructions below.
No   Continue with the Step #8 instructions below.

♦ ♦

Creating a new RSA exchange key

An application is creating a Protected item.

CryptoAPI Private Key

Security level set to Medium   [Set Security Level...]

[OK]   [Cancel]   [Details...]

8. Click on the [Set Security Level...] button.

♦ ♦

Importing a new private exchange key

Choose a security level appropriate for this item.

⊙ 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.

[< Back]   [Next >]   [Cancel]

9. Select the radio button for High (⊙ High). This will activate the password protection for your digital ID certificate.
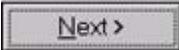
10. Select the [Next >] button to continue.

11. Enter the **new password twice**.
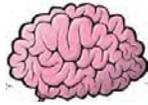
> **Note:**   *Commit to memory* this password as it will be needed every time you use your certificate. If a certificate password is forgotten, it cannot be reset. A new certificate must be requested. Since you are getting a new certificate during a renewal, you must again create a new certificate password. A minimum of 7 characters is recommended for your certificate password.
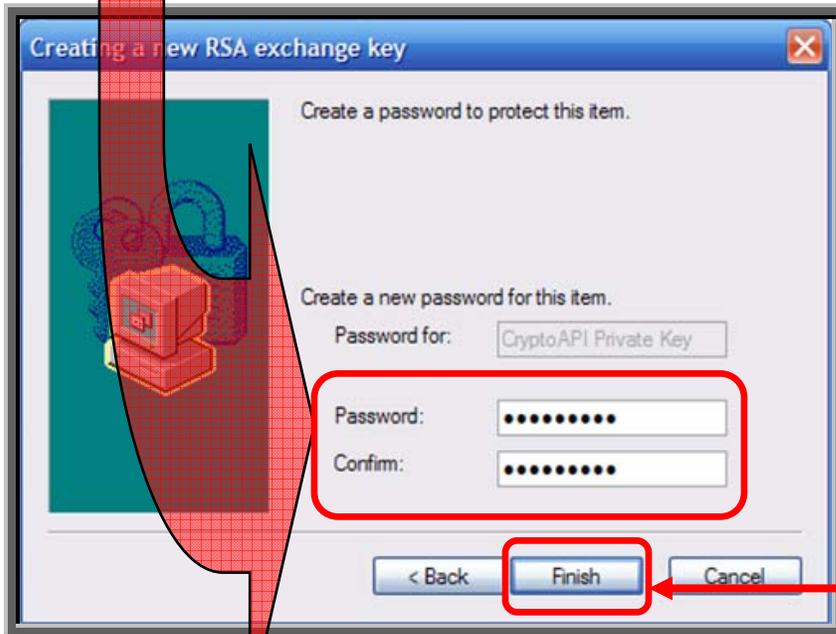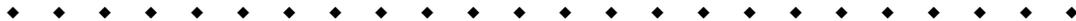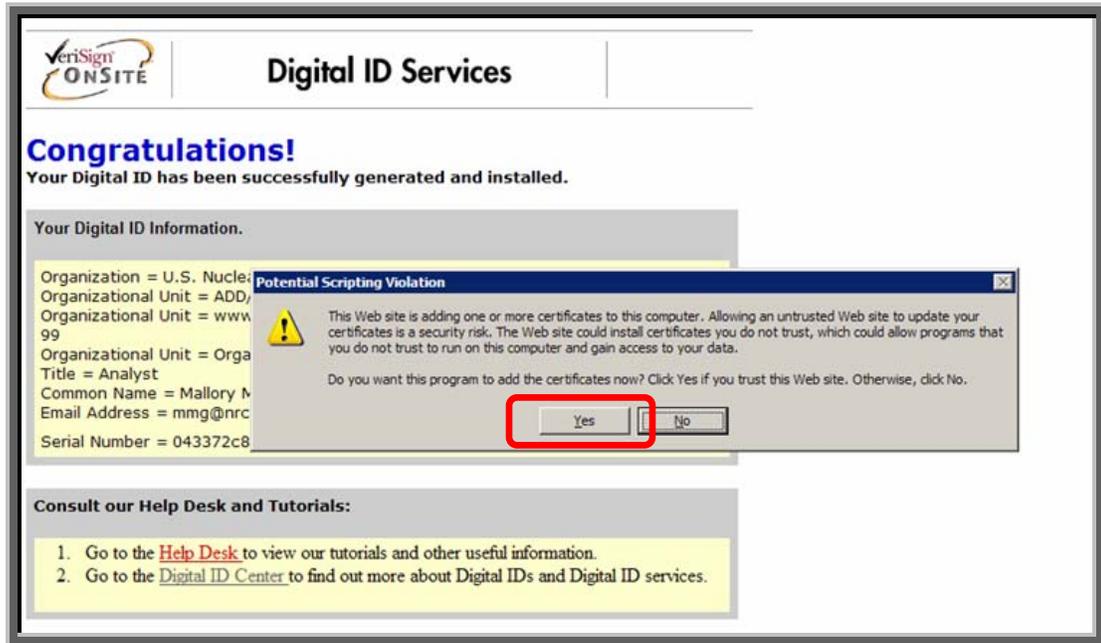

12. Select the **Finish** button.

13. Select the **OK** button, since the Security Level is set to High.

14. If you get a pop-up "**Potential Scripting Violation**" screen, select the [Yes] button to save your certificate to your computer. With Windows XP you are asked to verify that you want to install a digital certificate as shown below.
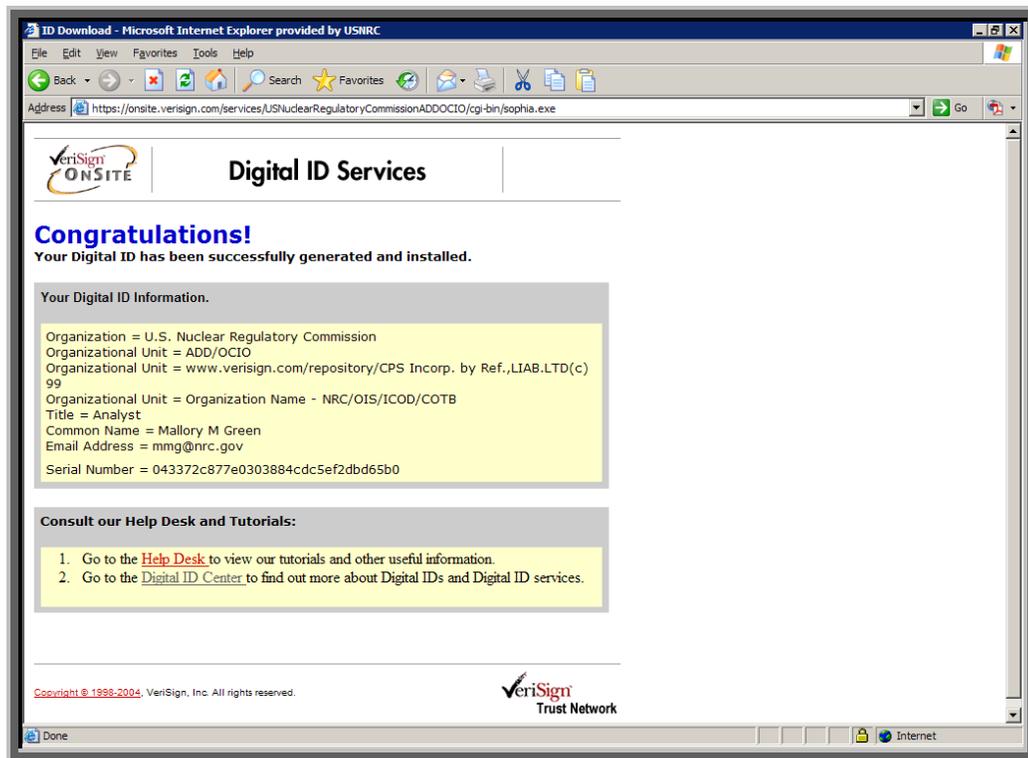
You will receive a **Congratulations!** screen telling you that your digital ID certificate have been successfully generated and installed.

12. Digital ID Certificate Revocations

The certificate owner must remember and use the Challenge Phrase which he or she chose during the certificate enrollment process in order to revoke his or her digital certificate. The steps to revoke your digital ID certificate are:

1. Click on the "**NRC's Digital ID Center**" link from either the "Electronic Submittals" web page or the "Obtain a Digital ID Certificate" web page.

2. Select the **REVOKE** option.

3. **Enter an appropriate email address or name** to search for the certificate you want to revoke and press the [Search] button.
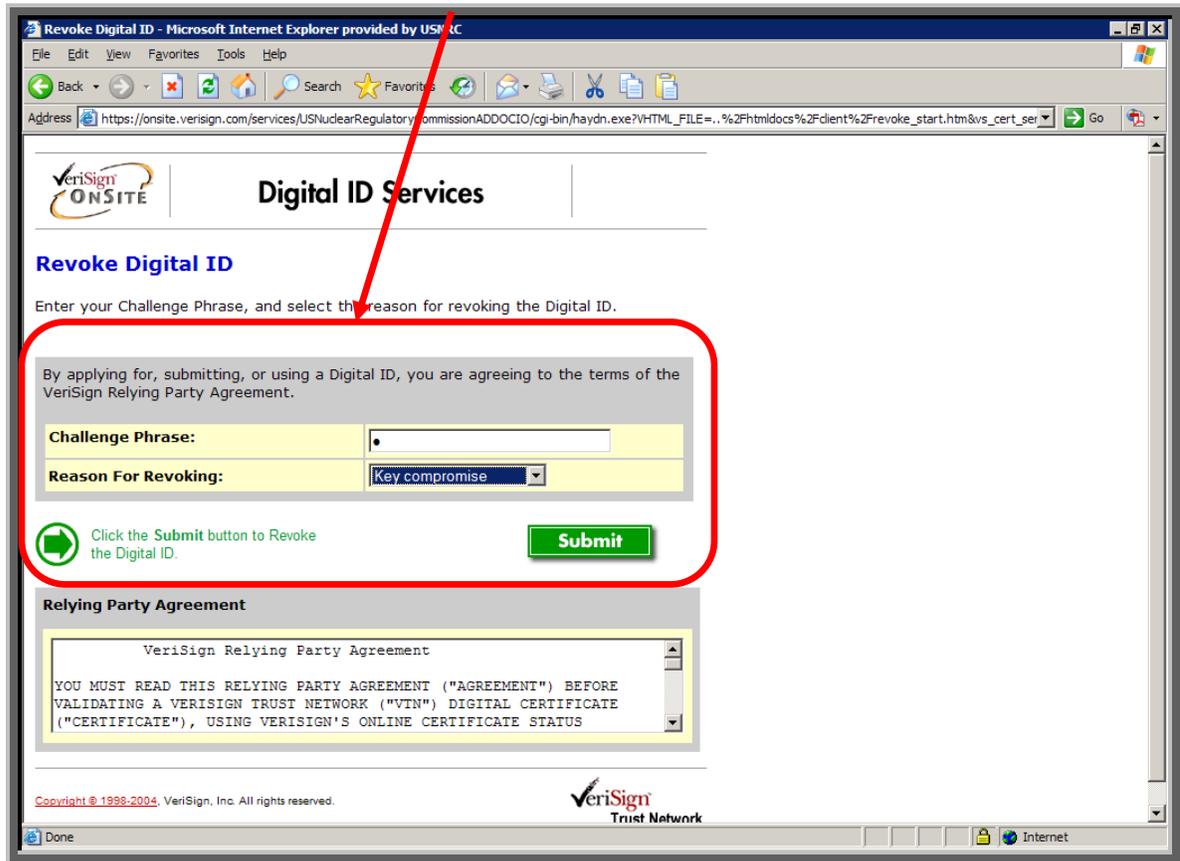

- -
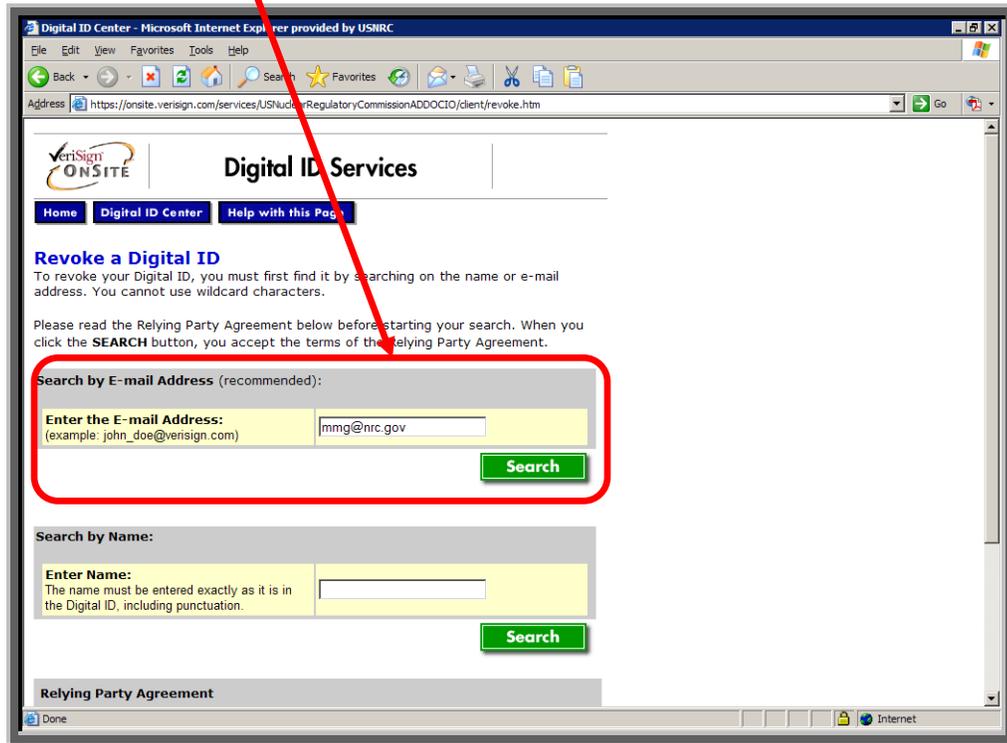
4. Select the applicable certificate you want to revoke.

5.   Review the data for the certificate you have chosen to revoke.

6.   Scroll down and click on the **Revoke** button to invalidate your certificate via VeriSign
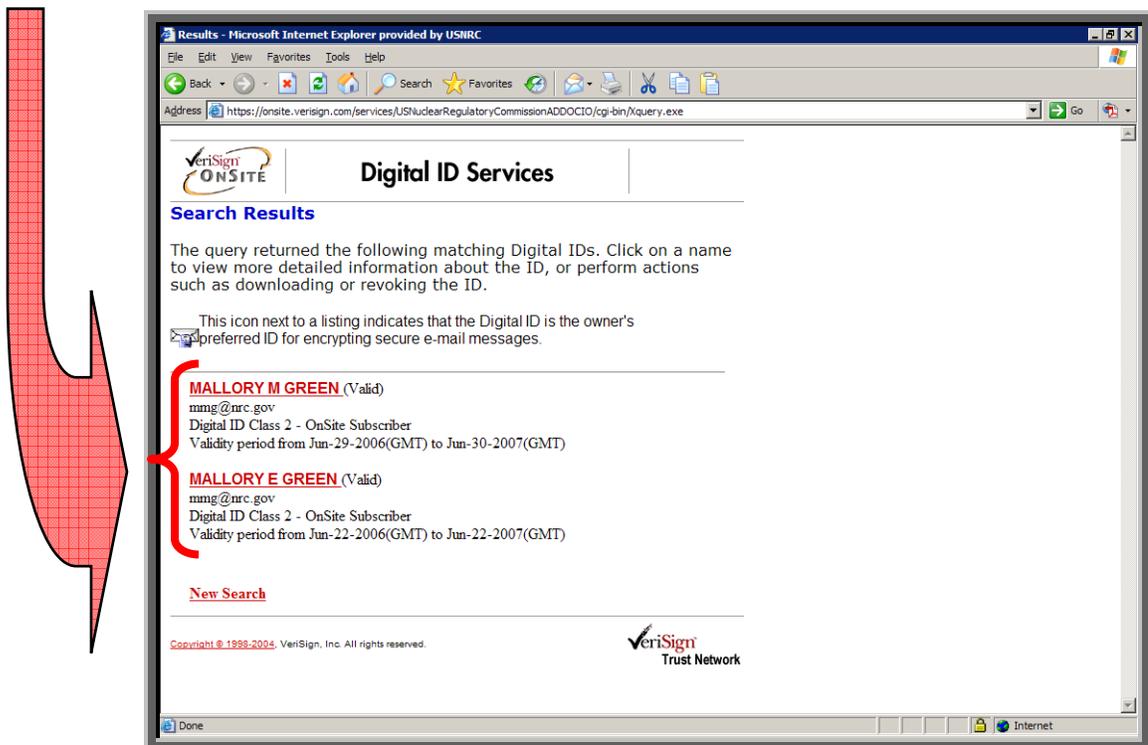
7. Enter the Challenge Phrase you entered during enrollment for this digital ID

certificate and then select the **Submit** button.

◆ ◆

8. Steps 1 – 7, above, made your certificate invalid, however, it did not remove the certificate from your PC, therefore follow Steps 1 – 4 within the Section 8, Digital ID Certificate Viewing Steps Instructions. After locating and selecting the certificate, to remove it from your PC, select the Remove button.