U.S. Nuclear Regulatory Commission
External Credentialing Service

NRC Digital Certificate
Activation Guide

Version 2.2

November 12, 2013
## Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Description</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>March 28, 2011</td>
<td>Initial draft</td>
<td></td>
</tr>
<tr>
<td>2.0</td>
<td>August 13, 2013</td>
<td>Updated to reflect new process</td>
<td></td>
</tr>
<tr>
<td>2.1</td>
<td>October 18, 2013</td>
<td>Added Install CA, updated screenshots</td>
<td></td>
</tr>
<tr>
<td>2.2</td>
<td>November 12, 2013</td>
<td>General Edits</td>
<td></td>
</tr>
</tbody>
</table>
Table of Contents

1. Introduction........................................................................................................................................3
2. Install the Root Certificate Authority..................................................................................................4
3. Credential Activation Process................................................................................................................12
4. Support..................................................................................................................................................22
1. Introduction

This document serves as a User Guide for the Nuclear Regulatory Commission (NRC) external partners that have a need to use NRC’s secure web based applications. More specifically, it describes the process through which an applicant activates a digital certificate.

Once the applicant has obtained a digital credential, it can be used to access NRC’s secure web based applications directly over the Internet.

The process of obtaining an NRC digital certificate consists of the following 2 high-level steps:

- Install the Root Certificate Authority
- Activate your NRC Credential
2. Install the Root Certificate Authority

1. Launch the Microsoft Internet Explorer web browser and navigate to the NRC External Credential Service (Level 1 Digital Certificates → https://pki.nrc.gov/Rudimentary). Click on Install CA.

2. Click on Save.
3. Save the file to a folder on your computer. Please make a note of this location. Click on Save.

4. Click on Close once the download is complete.

5. At the Microsoft Internet Explorer web browser, select Tools, then Internet Options.
6. Click on Contents, then on Certificates.
7. Click on Trusted Root Certification Authorities, then on Import.

8. Click on Next.
9. Click on Browse.

10. Browse to the location where the certificate file was saved. Select the file, and click on Open.
11. Click on Next.

12. Click on Next.
13. Click on Finish.

14. If the Security Warning dialog box is displayed, Click on Yes
15. Click on OK.

![Certificate Import Wizard]

The import was successful.
3. Credential Activation Process

This section takes the applicant through the activation process of a digital certificate. It assumes that the applicant has completed the credential enrollment process and has received the both the necessary approval and credential activation code. Each necessary screen is captured with an explanation of what the applicant is to comply with on each screen.

1. Prior to activating a digital certificate the user must have received the below notice indicating that they have been approved for a digital certificate. This email notification also includes the credential activation code that is required later in this process.

   ![Email Notification](image)

   **Subject:** Credential Request Approval Notification - eiegf test

   Dear eiegf test,

   Congratulations!

   Your request for a NRC Software Digital Certificate digital credential has been completely approved by the NRC.

   Your Approval Code is NRC2013064696188. Please have this with you as you will need this when in the process of activating your credential.

   - Please visit our website [NRC External Credential Service](#) to collect your certificate.
   - Once your credential has been collected you will be able to access the NRC application to which you requested access.

   Please note that your login for the NRC External Credential Service is ext0006. Please use the password selected by you during the initial request submission.

   Note: This is an auto-generated email from NRC External Credential Service. Please do not reply to this email.

   Thank you,

   NRC Identity, Credential, and Access Management Services

   **NOTE:** Please ensure that you’ve already followed the instructions in Section 2 (Install the Root Certificate Authority).

2. Launch the Microsoft Internet Explorer web browser and navigate to the NRC External Credential Service using the appropriate link provided in the above email to collect and activate your new digital certificate.
A. Level 1 Digital Certificates → https://pki.nrc.gov/Rudimentary

B. Level 3 Digital Certificates → https://pki.nrc.gov/Basic
3. To begin the activation process click on “Enroll”, then complete and submit the form as follows:

A. eMail Address – Enter your email address

B. NRC Approval Code – enter the approval code contained in the email notification you received as part of step 1 of this process.

C. Challenge Phrase – enter a challenge phrase that will be used by you to revoke your digital certificate in the future should you lose it.

D. Key Protection – check this box to protect your key

E. Submit – click the submit button
## 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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Your E-mail Address:</strong></td>
<td><a href="mailto:jdoe@verisign.com">jdoe@verisign.com</a></td>
</tr>
<tr>
<td><strong>NRC Approval Code:</strong></td>
<td>NRC20131316329912</td>
</tr>
</tbody>
</table>

### 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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enter Challenge Phrase:</strong></td>
<td>******</td>
</tr>
</tbody>
</table>

### 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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Check this Box to Protect Your Private Key</strong></td>
<td>✔️</td>
</tr>
</tbody>
</table>

### 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.

**Done**
Digital ID Subscriber Agreement
By applying for, submitting, or using a Digital ID, you are agreeing to the terms of the
VeriSign Subscriber Agreement.

SUBSCRIBER AGREEMENT
YOU MUST READ THIS SUBSCRIBER AGREEMENT ("SUBSCRIBER AGREEMENT")
BEFORE APPLYING FOR, ACCEPTING, OR USING A VERISIGN CERTIFICATE OR
DIGITAL ID ("CERTIFICATE" OR "DIGITAL ID"). IF YOU DO NOT AGREE TO
THE TERMS OF THIS SUBSCRIBER AGREEMENT, DO NOT APPLY FOR, ACCEPT,
OR USE THE CERTIFICATE.

1. Certificate Application and Description of Certificates. This
section details the terms and conditions regarding your application
("Certificate Application") for a Certificate and, if VeriSign
accepts your Certificate Application, the terms and conditions
regarding the use of the Certificate to be issued by VeriSign
to you as "Subscriber" of that Certificate. A Certificate is a
digitally signed message that contains a Subscriber's public key
and associates it with information authenticated by VeriSign or a
VeriSign-authorized entity. The Certificates provided under this
Agreement are issued within the VeriSign Trust Network ("VTN"). The
VTN is a global public key infrastructure that provides
Certificates for both wired and wireless applications. VeriSign is
one of the service providers within the VTN, together with a global
network of affiliates and partners throughout the world. The VTN
and VeriSign under this Agreement offer three distinct classes
("Classes") of certification services, Classes 1-3, for both the
wired and wireless Internet and other networks. Each level, or
class, of Certificate provides specific functionality and security
features and corresponds to a specific level of trust. You are
responsible for choosing which Class of Certificate you need. The
following subsections state the appropriate uses and authentication

4. Confirm your email address and click “OK”
5. On the “Creating a new RSA exchange key” prompt click “Set Security Level” then set the security level to “High” as indicated below. Click next to continue.
6. Create a Password to be used each time your certificate is required for authentication, then click “Finish”.

7. Confirm that the security level of your new digital certificate is now set to “High” and click “OK” to continue.
8. At this point the digital certificate is being created and installed into your certificate store. Do not stop or refresh your browser.

**Please wait while the Digital ID is being issued ...**

**NOTE:** Do not close your browser during this time or you will not receive your Digital ID. Also, do not press Stop or Refresh.
9. Follow these steps to confirm that your new digital certificate was installed correctly. From the Internet Explorer menu navigate to Tools → Internet Options → Content to display the below screen.
10. Click on Certificates button on the Internet Options → Content tab to display your certificate store. On the “Personal” tab, you should see a certificate “Issued by” the NRC. Select the certificate, and click on View.

11. Click on Certification Path. The path should be similar to the one shown below.
4. Support

Please visit the appropriate support resources for help and troubleshooting:


2. Application Support Desks
   a. Integrated Source Management Portfolio (ISMP)
      Phone: 877-671-6787
      eMail: ISMHelp.Resource@nrc.gov
   b. Electronic Filing (EIE)
      Phone: 866-672-7640
      eMail: Meta_System_Help_Desk.Resource@nrc.gov