

U.S. Nuclear Regulatory Commission

External Credentialing Service

NRC Digital Certificate Activation Guide

Version 2.2

November 12, 2013



Revision History

Version	Date	Description	Author
1.0	March 28, 2011	Initial draft	
2.0	August 13, 2013	Updated to reflect new process	
2.1	October 18, 2013	Added Install CA, updated screenshots	
2.2	November 12, 2013	General Edits	



Table of Contents

1.	Introduction	3
2.	Install the Root Certificate Authority	4
3.	Credential Activation Process	2
4.	Support2	2



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:





2. Install the Root Certificate Authority

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

Save As				×
Image: Arya, Avneesh > Downloads >		- 4 €	earch Downloads	Q
Organize 🔻 New folder			-	· ·
★ Favorites Name	Date modified	Туре	Size	
Desktop Downloads Recent Places	10/01/2013 1:43 PM	File folder		
 □ Libraries □ Documents □ Music □ Pictures □ Videos 				
P Computer ẫ (C:) OS ♀ (G:) ois (\\essays				
File <u>na</u> ne: FBCA-Root-SHA2.cer		_		
Hide Folders		C	Save	Cancel

4. Click on Close once the download is complete.

Download complete
Download Complete
FBCA-Root-SHA2.cer from pki.nrc.gov
Downloaded: 1.07KB in 1 sec
Download to: C:\Users\axa5\Dow\FBCA-Root-SHA2.cer Transfer rate: 1.07KB/Sec
Close this dialog box when download completes
Qpen Open Folder Close

5. At the Microsoft Internet Explorer web browser, select Tools, then Internet Options.





6. Click on Contents, then on Certificates.

Internet Options
General Security Trivacy Content Connectons Programs Advanced
Content Advisor Ratings help you control the Internet content that can be viewed on this computer.
Petings
Certificates
Use certificates for encrypted connections and identification.
Clear SSL state Certificates Publishers
AutoComplete
AutoComplete stores previous entries Settings on webpages and suggests matches for you.
Feeds and Web Slices
Feeds and Web Slices provide updated Settings content from websites that can be read in Internet Explorer and other programs.
Some <u>settings</u> are managed by your system administrator.
OK Cancel Apply



7. Click on Trusted Root Certification Authorities, then on Import.

Certificates				
Intended purpose: <a>				
Intermediate Certification Au	ithor ties Trusted Root Co	ertification Aut	horities Trusted Publ	
Issued To	Issued By	Expiratio	Friendly Name	
AAA Certificate Ser ABA.ECOM Root CA AC Raíz Certicámar AC RAIZ DNIE AC RAIZ FNMT-RCM AC 1 RAIZ MTIN ACEDICOM Root A-CERT ADVANCED ACNLB	AAA Certificate Services ABA.ECOM Root CA AC Raíz Certicámara AC RAIZ DNIE AC RAIZ FNMT-RCM AC1 RAIZ MTIN ACEDICOM Root A-CERT ADVANCED ACNLB	12/31/2028 07/09/2009 04/02/2030 02/08/2036 12/31/2029 11/03/2019 04/13/2028 10/23/2011 05/15/2023	COMODO DST (ABA.ECOM AC Raíz Certicá DIRECCION GEN AC RAIZ FNMT AC1 RAIZ MTIN EDICOM A-CERT ADVANC NLB Nova Ljublja	
Import	<u>R</u> emove		Advanced	
ee anexe mended parpose			View	
Learn more about <u>certificates</u> Close				

8. Click on Next.

Certificate Import Wizard	×
	Welcome to the Certificate Import Wizard
<u>F</u>	This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
~	A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
	To continue, dick Next.
	< Bad Next > Cancel



9. Click on Browse.

Certificate Import Wizard
File to Import Specify the file you want to import.
Eile name:
Note: More than one certificate can be stored in a single file in the following formats:
Personal Information Exchange- PKCS #12 (.PFX,.P12)
Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
Microsoft Serialized Certificate Store (.SST)
Learn more about <u>certificate file formats</u>
< <u>B</u> ack <u>N</u> ext > Cancel

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

6 Open					×
🚫 🗸 🖡 🕨 Arya, Avne	eesh 🕨 Downloads 🕨		🔹 🗲 Search	Downloads	Q
Organize 🔻 New folder	r			== -	
☆ Favorites	Name	Date modified	Туре	Size	
📃 Desktop	🕌 VSphere	10/01/2013 1:43 PM	File folder		
🐌 Downloads	FBCA-Root-SHA2.cer	10/17/2013 3:54 PM	Security Certificate	2 KB	
📃 Recent Places					
🥃 Libraries 😑					
Documents					
J Music					
Pictures					
Videos					
Computer					
(0.) ois (((inc.go					
(N) VIEW (()					
T (1) HVHD ((())(C) +					
File <u>n</u> a	me: FBCA-Root-SHA2.cer		× X.509 Ce	rtificate (".ce <mark>r</mark> ;*.	crt) 🔻
			Oper		ancel



11. Click on Next.



12. Click on Next.

Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for the certificate.
\bigcirc Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Certificate store:
Trusted Root Certification Authorities Browse
Learn more about <u>certificate stores</u>
< Back Next > Cancel



13. Click on Finish.



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





15. Click on OK.

Certificate Import Wizard	J
The import was successful.	
ОК	



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.



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

 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 \rightarrow <u>https://pki.nrc.gov/Rudimentary</u>



B. Level 3 Digital Certificates \rightarrow <u>https://pki.nrc.gov/Basic</u>

13





- 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



VeriSign Enro	eriSign Enrollment				
Help with this Page					
Complete Enrollment Form					
Enter your Digital ID information					
Fill in all required fields. Fields marked with an a are viewable in the certificate's details.	asterisk (*) are included with your Digital ID and				
Your E-mail Address: * (required) (example jbdoe@verisign.com)	ecsl1.test@ft.ctf.nrc.gov				
NRC Approval Code: (required)	NRC20131316325912				
Digital ID. Do not share it with anyone. Do not lo renew your Digital ID. Enter Challenge Phrase: (required) Do not use any punctuation.	se it. You will need it when you want to revoke or				
Enter Challenge Phrase: (required) Do not use any punctuation.	•••••				
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					
Optional: Enter Comments In some cases, your administrator will instruct y to you and the administrator) in this field. The au really is you submitting the application. This cor	rou to enter <i>Shared Secret</i> information (known only dministrator uses this shared secret to verify that it nment will not be included in your Digital ID.				
ne					



 SUBSCRIBER AGREEMENT YOU MUST READ THIS 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. 	he
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 your 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 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	I
If all the information above is correct, click Submit to continue. Submit Cancel 1008. VeriSign, Inc. All rights reserved.	Sign

4. Confirm your email address and click "OK"



Message	from webpage
2	Confirm your e-mail address: ecsl1.test@ft.ctf.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

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.

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 <u>D</u> etails	



Creating a new RSA exch	ange key	×
	Choose a security level appropriate for this item.	
	 High Request my pemission with a password when this item is to be used. Medium Request my pemission when this item is to be used. 	
	< Back Next > Cancel	

6. Create a Password to be used each time your certificate is required for authentication, then click "Finish".

Creating a new RSA exch	ange key	X
	Create a password to protect this item.	
	Create a new password for this item. Password for: CryptoAPI Private Key Password: ••••••• Confirm: •••••••	
	< Back <u>F</u> inish Ca	ncel

7. Confirm that the security level of your new digital certificate is now set to "High" and click "OK" to continue.



Creating a new	RSA exchange key	×
	An application is creating a Protected item.	
	CryptoAPI Private Key	
	Security level set to High Set <u>Security Level</u>]

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 ${\bf Stop}$ or ${\bf Refresh}.$





ongratula our Digital ID has be	tions! een successfully generated and in	nstalled.
our Digital ID Informa	tion.	
Country = US Drganization = U.S. N Drganizational Unit = Common Name = Ecs 2_08081323070765	luclear Regulatory Commission External 2803A middle test 54	
Serial Number = 2bd5	b40042bae8111418804aa93becac	
onsult our Help De	sk and Tutorials:	
 Go to the <u>Help D</u> Go to the <u>Digital</u> 	<u>esk</u> to view our tutorials and other usefi ID Center to find out more about Digita	iul information. Il IDs and Digital ID services.

9. Follow these steps to confirm that your new digital certificate was installed correctly. From the Internet Explorer menu navigate to Tools \rightarrow Internet Options \rightarrow Content to display the below screen.

Internet Op	tions				? ×
General S	ecurity Privacy	Content	Connection	ns Program	s Advanced
Content A	dvisor Ratings help you viewed on this c	i control the omputer.	e Internet o	ontent that o	an be
Certificate	use certificates	for encrypt	ed connecti	ons and iden	tification.
Cle	ear <u>S</u> SL state	<u>C</u> ertif	icates	Publis	hers
AutoComp	lete				
	AutoComplete stores previous entries Settings for you.				
Feeds and	Web Slices				
	Feeds and Web content from we read in Internet programs.	Slices provi bsites that Explorer an	de updated can be id other	Sett	ings
		ОК		Cancel	Apply



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.

Certificates			?
Intended purpose:	<all></all>		1
Personal Other Peopl	e Intermediate Certification	Authorities Trus	ted Root Certification
Issued To	Issued By	Expiratio	Friendly Name
Ecs0803A middle	test NRC Rudimentary CA (52 8/6/2016	<none></none>
Import	ort <u>R</u> emove		<u>A</u> dvanced
Certificate intended pu	rposes		
<all></all>			<u>V</u> iew
			Close

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

Certificate	×
General Details Certification Path	
Certification path	
Federal Bridge CA	
NRC Rudimentary CA G2	
	View Certificate
Certificate status:	
This certificate is OK.	
Learn more about <u>certification paths</u>	
	OK



4. Support

Please visit the appropriate support resources for help and troubleshooting:

- 1. User Guides located at <u>https://pki.nrc.gov/ecs/guides.html</u>
- 2. Application Support Desks
- a. Integrated Source Management Portfolio (ISMP)
 Phone: 877-671-6787
 eMail: ISMPHelp.Resource@nrc.gov
- b. Electronic Filing (EIE)
 Phone: 866-672-7640
 eMail: Meta_System_Help_Desk.Resource@nrc.gov