

Introduction

The following guide will take you through the process of downloading your Public Key Infrastructure (PKI) certificate. Before you download the PKI certificate, you must first meet with the Local Registry Authority (LRA) or Trusted Agent assigned to your site. This person is responsible for verifying your identity and submitting your personal information, and once this is complete, the LRA will present you with a Certificate Registration Instruction (CRI) document. The CRI will contain important information necessary for downloading your PKI certificate. Once you have received your CRI from your LRA, you are ready to download your certificate.

How to download your certificate

1. Using Netscape Navigator version 4.5 or newer? Go to either <http://reg.c3pki.den.disa.mil> or <http://reg.c3pki.chamb.disa.mil>.
2. Read the information on the User Registration Page, and click Next>.
NOTE: Depending on which certificates are installed on your machine, you may not see steps 3-6.
3. A window will appear. Read the information and click Next>.
4. Read the information in the next window, and click Next>.
5. Select Accept this certificate for this session in the next window, and click Next>.
6. Do NOT click the checkbox in the next window and click Next>.
7. You will get the message: *You have finished examining the certificate presented by:ca-1chamb.disa.mil.* in the next window. Click Finish.
8. The Security Information window displays. Check the Show this Alert Next Time box and click Continue.
9. This will bring you back to the User Registration page, click Download Class 3 Root CA Certificate.
NOTE: If you get a message that this certificate has already been installed, proceed to step 17.
10. Read the information in the window and click Next>.
11. Read the information in the window and click Next>.
12. Click More Info... in the next window.
13. Compare the Certificate Fingerprint with the fingerprint on your CRI. If the number is different, stop and notify your LRA. If they are the same, click OK and then Next>.
14. Check all three boxes and click Next> in the next window.
15. Do NOT click the checkbox in the next window and click Next>.
16. Type DOD PKI Class 3 Root in the next window and click Finish.
17. This will bring you back to the User Registration page, click Download Medium Assurance Root CA Certificate.
NOTE: If you get a message that this certificate has already been installed, proceed to step 25.
18. Read the information and click Next> in the next window.
19. Read the information and click Next> in the next window.
20. Click More Info... in the next window.
21. Compare the Certificate Fingerprint with the fingerprint on your CRI. If the number is different, stop and notify your LRA. If they are the same, click OK and then Next>.
22. Check all three boxes and click Next> at the next window.
23. Do NOT click the checkbox in the next window,, and click Next>.
24. Type DOD PKI Med Assurance and click Finish in the next window.
25. This will bring you back to the User Registration page, click Next>.
26. Click the CA shown on your CRI form at the next screen.

Note: Additional screens may be displayed during the afternoon hours while accessing this site. These screens are outlined in Steps 27 to 31. If you do not see these screens, go to Step 32.

27. Review the information on the screen and click Next>.
28. Review the information on the screen and click Next>.
29. Select Accept this certificate for this session in the next window, and click Next>.
30. Do NOT click the checkbox in the next window and click Next>.
31. You will get the message: *You have finished examining the certificate presented by:ca-1chamb.disa.mil* in the next window. Click Finish.
32. Enter the User Number from your CRI, and click Submit Request.
33. Enter the Access Code from your CRI, and click Submit Request.
34. Click OK at the next window,.

NOTE: If a password is already configured, you will go directly to step 37.

35. Create a password in the next window, that is at least eight characters, contains both upper and lower case letters, at least one number, and no words or names. This password will protect all keys placed in the Netscape Communicator database. Then click OK.

NOTE: The next window that appears will notify you that the Certificate Request is being generated. Please wait. When this window disappears, your certificate has been successfully acquired.

36. The DoD Class 3 PKI User Registration Page displays.
37. Click the Security button in the Netscape toolbar.
38. In the Security Info window, under Certificates, click Yours.
39. Highlight your certificate and click Export.
40. Enter your password and click OK.
41. Enter your password and click OK.
42. Confirm the password and click OK.
43. Insert a floppy disk into your computer.
44. Select 3 1/2 Floppy (A:) from the Save in: drop down list and enter a name for your certificate in the File name: field. Click Save.
45. A confirmation message window will appear. Click OK.
46. Click Cancel to close the Your Certificates Window.
47. Close your Netscape window.

Loading your PKI certificate into your NMCI laptop

When you receive your NMCI Laptop, you must copy your certificate from your floppy disk onto the hard drive on your machine. Perform the steps:

1. Insert your PKI floppy disk into your machine.
2. Browse the floppy disk drive. Highlight your certificate by right clicking on it, and select Copy from the menu that appears.
3. Locate the Certs folder on your NMCI machine through the following paths:
C:/Program Files/Alcatel/Certs OR C:/Program Files/Timestep/Certs
NOTE: If no Certs folder exists, create one and proceed to the next step.
4. Open this folder, right click in the window and select Paste.

In Closing

For further instructions on Remote Access Service (RAS) go to:

<http://www.nmci-isf.com/userinfo.htm>

The PKI certificate will also provide you the opportunity to read email from a non-NMCI workstation via the Internet using Outlook Web Access.