FREQUENTLY ASKED QUESTIONS - Customer Partner Access Registration

- *Who do I contact if I have a question or problem with registration?*

  Contact your Northrop Grumman program contact/sponsor. Refer to the signature block of the "Invitation to Collaborate with Northrop Grumman" you received if you need contact information details (do not reply to the invitation email).

- *What should I do if I just received an invitation, but I already collaborate with Northrop Grumman on a different program?*

  Since you were already issued an external partner account by Northrop Grumman (NG) to access sites/applications, you do not need another account for the new program. Send an email to your NG program contact or sponsor (refer to the signature block of the "Invitation to Collaborate with Northrop Grumman" email you just received) and inform them that you already have an NG partner account; they can add your existing account to the new program. Do not complete the registration unless you are told to do so after informing them you already have an account (registration may be needed if your current account is no longer active or if your account requires new information).

- *Do I need a certificate to be able to collaborate with Northrop Grumman?*

  No; your Northrop Grumman (NG) program contact/sponsor will request that NG remote access will be issued to you for logging on.

- *What do I do if the certificate I currently have does not appear on the **Certificate Issuer** dropdown on the "Authentication Method" page?*

  Send your exported certificate (see instructions below in "Exporting Certificate" section) to your Northrop Grumman (NG) program contact/sponsor (found in signature block of invitation email) via email. They will submit it for approval to determine if the certificate can be used. Note: If you see the same name on the dropdown, but a different number, you will still need to send your exported certificate to get it approved.

  If your certificate type will not be approved, your NG program contact/sponsor will request that NG remote access will be issued to you for logging on.

- *How do I know what value to enter for my certificate?*

  Certificate information used by Northrop Grumman (NG) must be unique and match exactly (it is case sensitive) what is on your certificate. In most cases, the unique value can be found in the **Subject** field on the **Details** tab of the certificate (see instructions below in "Getting Certificate Information" section).

  Some certificates use the **Subject Alternative Name** field on the **Details** tab instead. In registration, after you have selected your certificate from the dropdown, the instructions on the screen will tell you when to use the **Subject Alternative Name** field. Listed below are the currently approved certificates that use the **Subject Alternative Name** field.

Certificate Issuer/Certificate Authority	**Value from Certificate in Subject Alternative Name**
HHS-FPKI-Intermediate-CA-E1	Other Principal Name
Lockheed Martin US Certification Authority-2	Other Principal Name
Lockheed Martin Certification Authority 4 G2	Other Principal Name
NASA Operational CA	Other Principal Name
Raytheon class3	Other Principal Name
Raytheon Class 3 MASCA	Other Principal Name
U.S. Department of State PIV CA	Other Principal Name
U.S. Department of Transportation Agency CA G4	Other Principal Name
Booz Allen Hamilton CA 02	RFC822 Name
Carillon PKI Services CA 1	RFC822 Name
DHS CA4	RFC822 Name
Entrust Managed Services SSP CA	RFC822 Name
IdenTrust ACES CA 2	RFC822 Name
Symantec Client External Certification Authority - G4	RFC822 Name
VeriSign Client External Certification Authority - G2	RFC822 Name
VeriSign Client External Certification Authority - G3	RFC822 Name
WidePoint ORC ECA 7	RFC822 Name

Note: The value you enter during registration is exported to your NG partner account. If the value in the partner account does not match the value on your certificate exactly, you will not be able to logon. If you entered incorrect information during registration, once your partner account is created, you will need to send your certificate information (see instructions below in "Exporting Certificate" section) to your NG program contact/sponsor and they can update the information for you.

- *What is the difference between the addresses on the "Company Information", "Business Mailing Address", and "Shipping Address" pages?*

  The address you enter on the "Company Information" page is the corporate address of your company. If you do not know the corporate address, you can enter your local business mailing address.

  The address you enter on the "Business Mailing Address" page is the address of where you are located. If this address is the same as the corporate address, you should check off the **Use Company Address** box. You will not need to enter the address again. If your local business mailing address is different than your company's corporate address, enter your local business mailing address on this page.

  If you do not have a certificate to use to log in (e.g. DOD CAC, Exostar, etc.), your Northrop Grumman (NG) program sponsor will request that you be set up with NG remote access.

  - If you do not have a smartphone, a physical token is needed and will be sent to you. If you entered a PO Box as your business mailing address, you are required to enter a physical address (no PO boxes) for your address on the "Shipping Address" page.

  If you are using a certificate to log in, you do not need to enter an address on the "Shipping Address" page and can click the **Skip** button.

EXPORTING CERTIFICATE

Export your certificate to a file by following these steps for your browser:

Edge

1. Click 3 dots (**…**) at top right
2. Select **Settings** from menu
3. Select **Privacy, search, and services** on left
4. Scroll down and select **Manage certificates** in **Security** section
5. On **Personal** tab, click on the certificate to be used to login
   - If more than one certificate is displayed, click each certificate and look at **Certificate intended purposes**. Select the certificate that has **Smart Card Logon** and/or **Client Authentication** listed. Note: One with Smart Card Logon is preferred over one with just Client Authentication.
   - Verify that the certificate is not expired
   - If Exostar is the Issuer, select the one that contains "(Identity)"
6. Click **Export** button
7. Click **Next** when "Certificate Export Wizard" dialog box appears
8. Select **No, do not export the private key**, then click **Next**
9. Select **DER encoded binary X.509 (.CER)**, then click **Next**
10. Click **Browse**
11. Click "Desktop" (or another location that you can find when attaching a file to email)
12. Enter *Lastname*.ngcer in **File name** (e.g., Smith.ngcer)
13. In **Save as type** dropdown, select **All Files (*.*)**, then click **Save**
    Note location (folder) of the file being created
14. Click **Next**
15. Click **Finish**
16. Click **OK**
17. Click **Close** for "Certificates" dialog box
18. Close **Settings** tab in browser
19. Attach export file as attachment in email
    If .CER files are restricted, rename the file to remove the ".CER" portion of the file (e.g., Smith.ngcer).

Internet Explorer

1. Select **Tools** menu
2. Select **Internet Options**
3. Select **Content** tab
4. Click **Certificates** button
5. Select **Personal** tab
6. Click on the certificate to be used to login
   - If more than one certificate is displayed, click each certificate and look at **Certificate intended purposes**. Select the certificate that has **Smart Card Logon** and/or **Client Authentication** listed. Note: One with Smart Card Logon is preferred over one with just Client Authentication.
   - Verify that the certificate is not expired
   - If Exostar is the Issuer, select the one that contains "(Identity)"

7. Click **Export** button
8. Click **Next** when “Certificate Export Wizard” dialog box appears
9. Select **No, do not export the private key**, then click **Next**
10. Select **DER encoded binary X.509 (.CER)**, then click **Next**
11. Click **Browse**
12. Click “Desktop” (or another location that you can find when attaching a file to email)
13. Enter *Lastname*.ngcer in **File name** (e.g., Smith.ngcer)
14. In **Save as type** dropdown, select **All Files (*.*)**, then click **Save**
    Note location (folder) of the file being created
15. Click **Next**
16. Click **Finish**
17. Click **OK**
18. Click **Close** for “Certificates” dialog box, then click **OK**
19. Attach export file as attachment in email
    If .CER files are restricted, rename the file to remove the “.CER” portion of the file (e.g., Smith.ngcer).

GETTING CERTIFICATE INFORMATION

Here are steps to get information from your certificate and enter into CPA registration:

Edge

1. Click 3 dots (**…**) at top right
2. Select **Settings** from menu
3. Select **Privacy, search, and services** on left
4. Scroll down and select **Manage certificates** in **Security** section
5. On **Personal** tab, click on the certificate to be used to login
    - If more than one certificate is displayed, click each certificate and look at **Certificate intended purposes**. Select the certificate that has **Smart Card Logon** and/or **Client Authentication** listed. Note: One with Smart Card Logon is preferred over one with just Client Authentication.
    - Verify that the certificate is not expired
    - If Exostar is the Issuer, select the one that contains “(Identity)”
6. Select **View** to examine the certificate you selected above
7. Select **Details** tab
8. Note the **Issuer** on the certificate; select this in the **Certificate Issuer** selection in CPA registration
9. Note the **Valid To** on the certificate; enter this date in **Valid To** date entry in CPA registration
10. While on the **Details** tab, click on **Subject** or **Subject Alternative Name** in the **Field** column
    Based on what was selected in **Certificate Issuer** in CPA registration, CPA will display which one needs to be used (Subject or Subject Alternative Name)
11. Highlight with your mouse all the data in the lower pane of the dialogue box below and copy it (keystroke: Ctrl-C)
12. Click **OK**, **Close**, and exit **Settings** tab; return to CPA registration
13. Paste the data you copied (keystroke: Ctrl-V) into the **Subject** or **Subject Alternative Name** entry field below

Internet Explorer

1. Select **Tools** menu
2. Select **Internet Options**
3. Select **Content** tab
4. Click **Certificates** button
5. On **Personal** tab, click on the certificate to be used to login
    - If more than one certificate is displayed, click each certificate and look at **Certificate intended purposes**. Select the certificate that has **Smart Card Logon** and/or **Client Authentication** listed. Note: One with Smart Card Logon is preferred over one with just Client Authentication.
    - Verify that the certificate is not expired
    - If Exostar is the Issuer, select the one that contains "(Identity)"
6. Select **View** to examine the certificate you selected above
7. Select **Details** tab
8. Note the **Issuer** on the certificate; select this in the **Certificate Issuer** selection in CPA registration
9. Note the **Valid To** on the certificate; enter this date in **Valid To** date entry in CPA registration
10. While on the **Details** tab, click on **Subject** or **Subject Alternative Name** in the **Field** column
    Based on what was selected in **Certificate Issuer** in CPA registration, CPA will display which one needs to be used (Subject or Subject Alternative Name)
11. Highlight with your mouse all the data in the lower pane of the dialogue box below and copy it (keystroke: Ctrl-C)
12. Click **OK**, **Close**, and **OK**; return to CPA registration
13. Paste the data you copied (keystroke: Ctrl-V) into the **Subject** or **Subject Alternative Name** entry field below