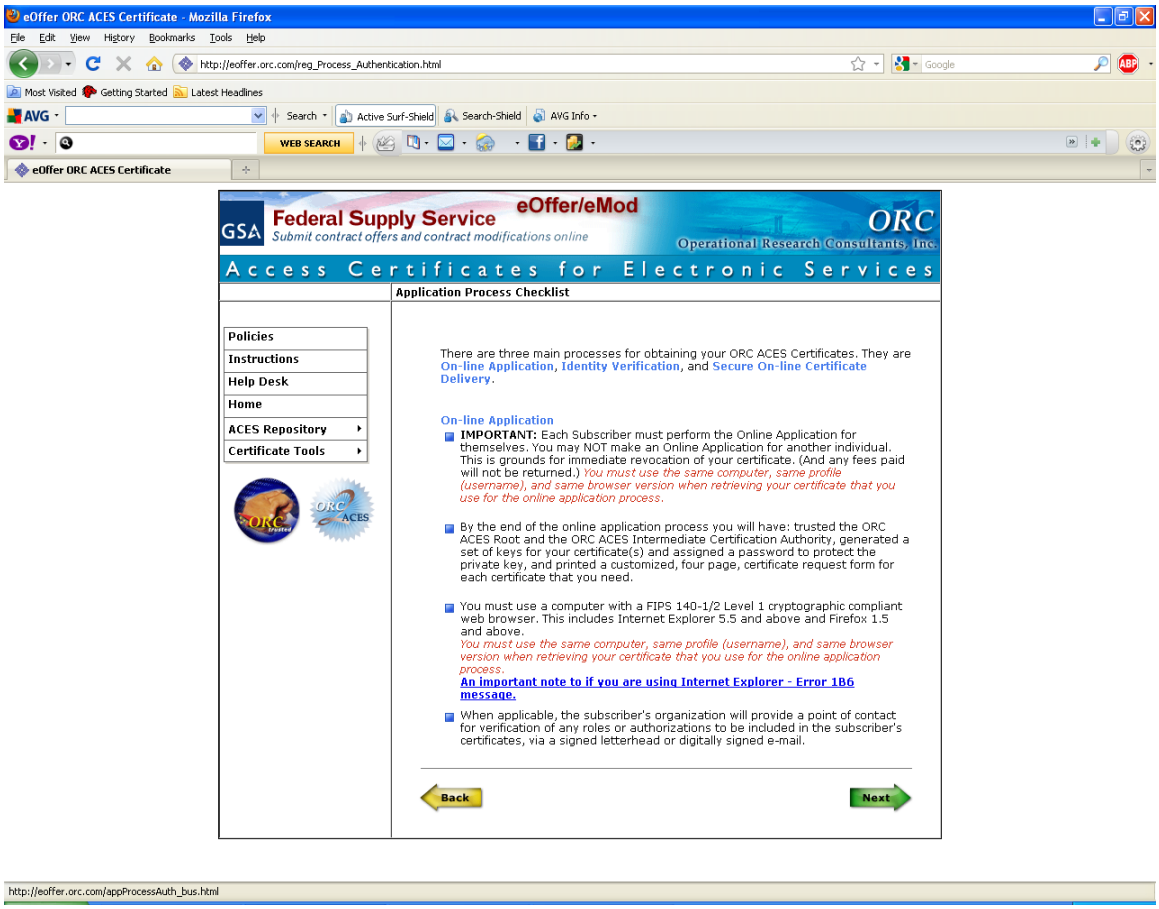
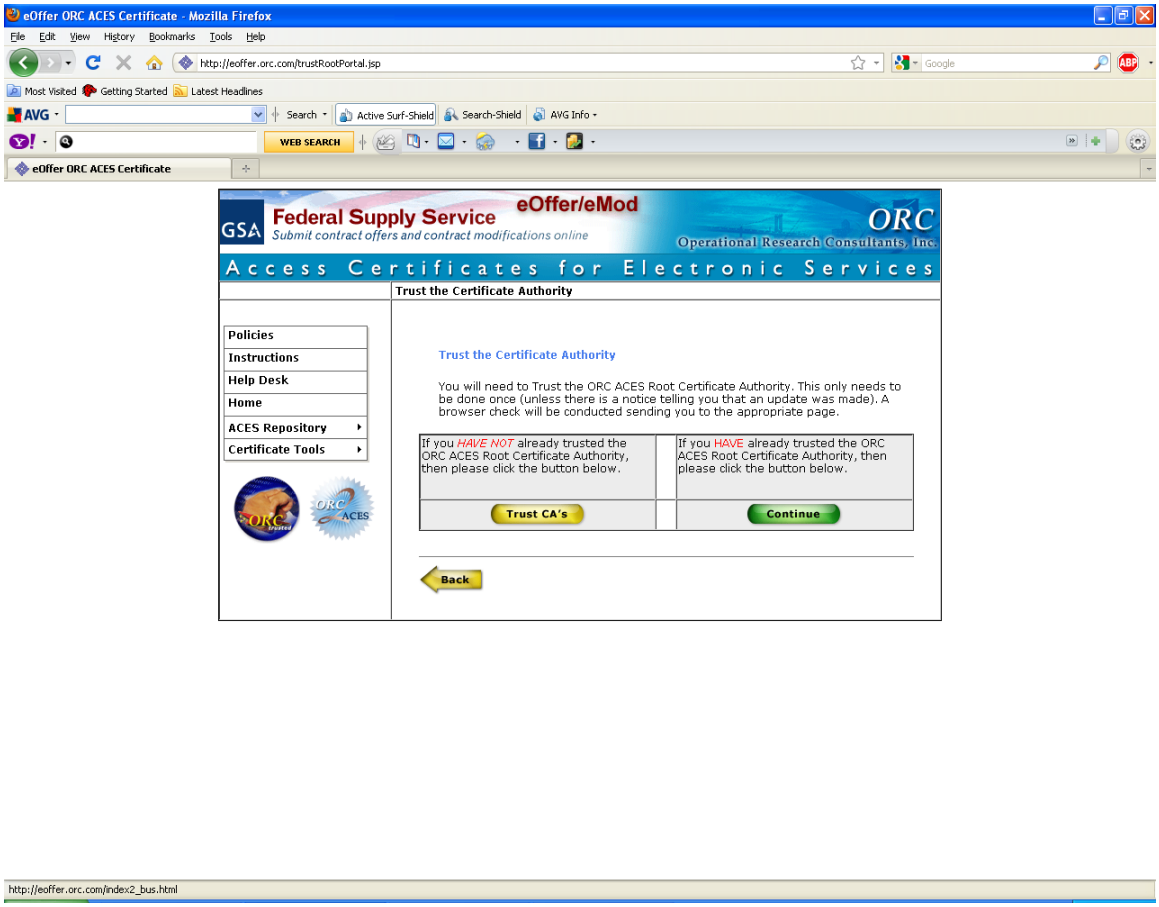
Instructions for ACES-Business identity certificate request process on the ORC ACES website for GSA eOffer users (Mozilla Firefox users on Windows)

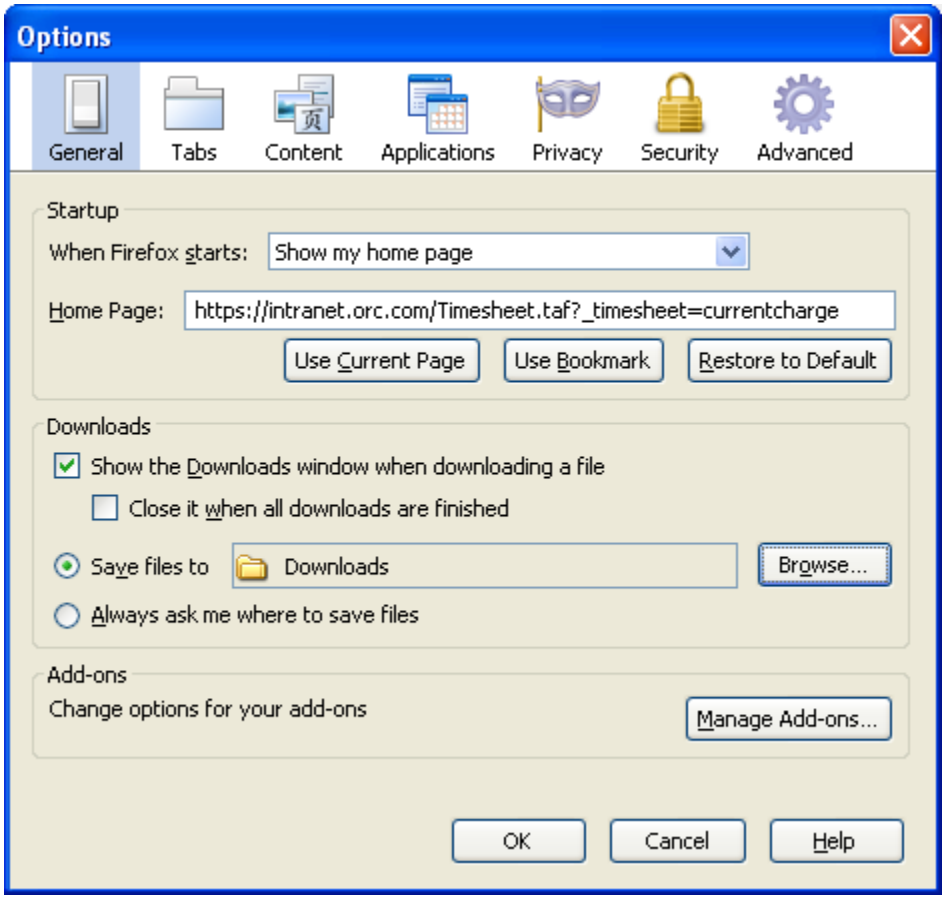
Click the green **Next** arrow to get started and click on the green **Next** arrow on the following pages.



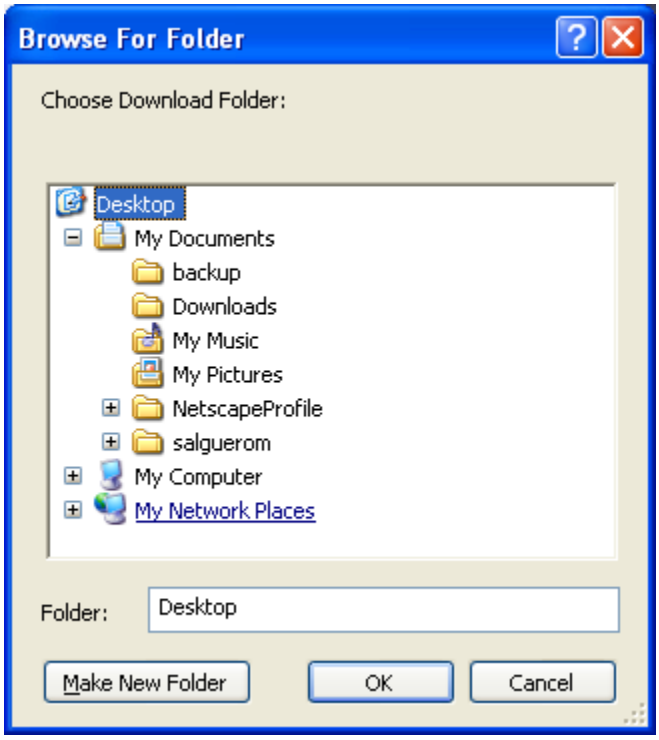
Stop at the **Trust the Certificate Authority** page. If this is your first time applying for an ACES-Business identity certificate, you must click the **Trust CA**s button in order to download the ACES Root and signing certificate files.



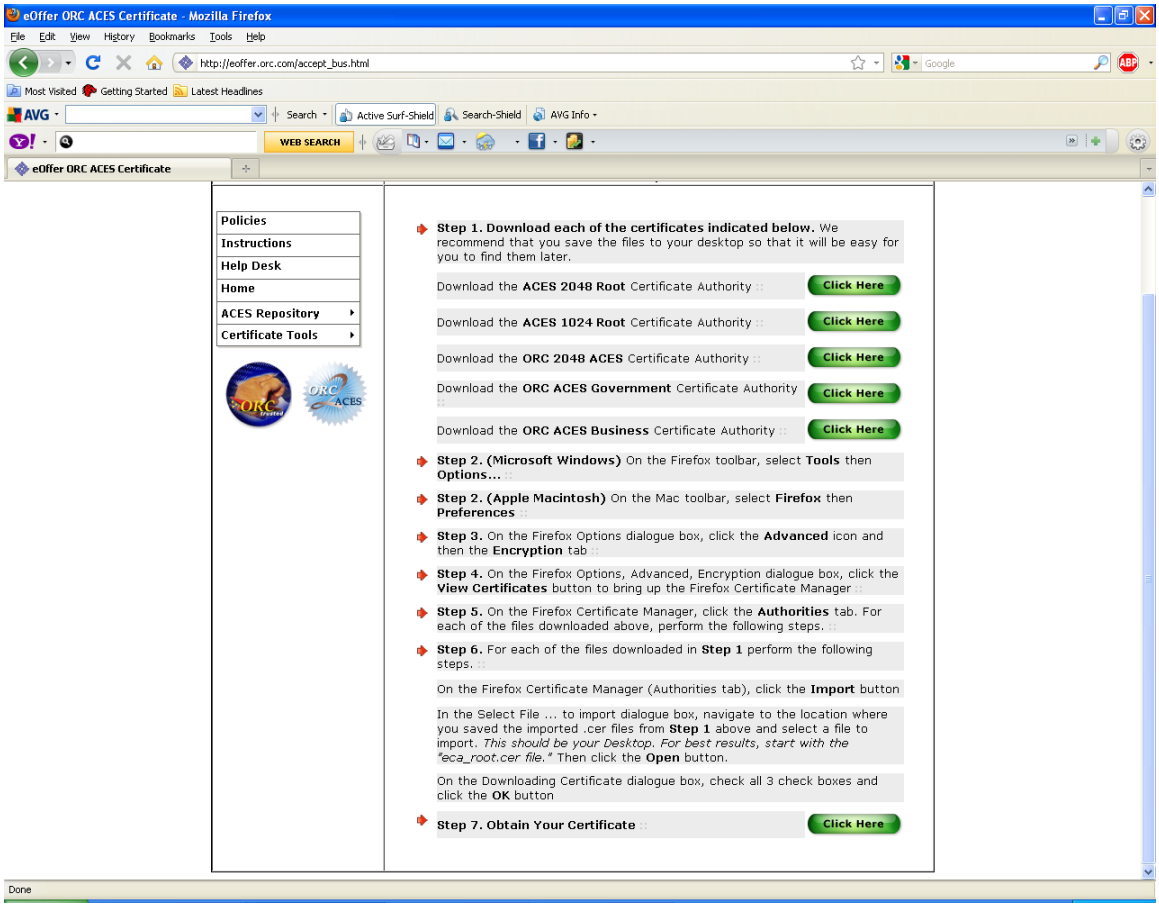
In order to ensure that all of the ACES Root and signing certificate files are downloaded to your Desktop, select **Tools**, select **Options**, and select **General** icon.



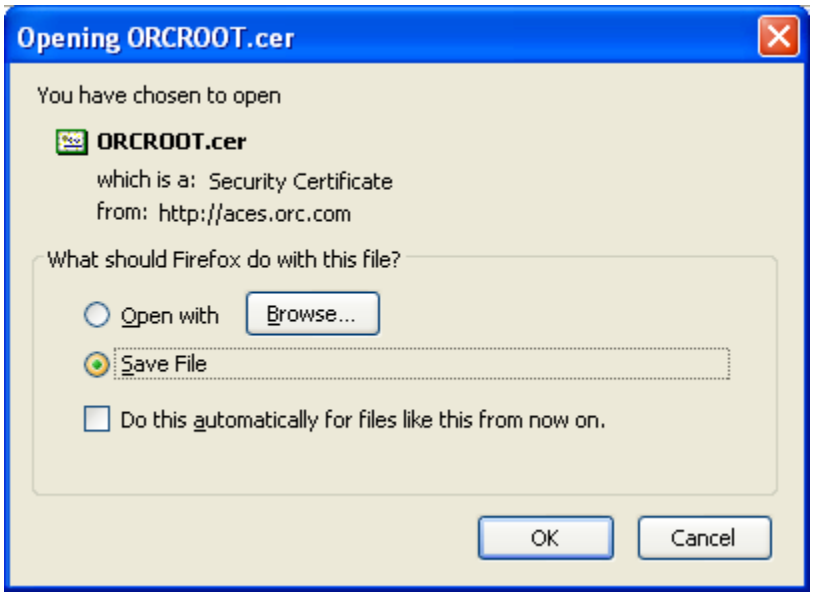
After clicking on **Browse** next to **Save files to Downloads**, select **Desktop** and click **OK**.



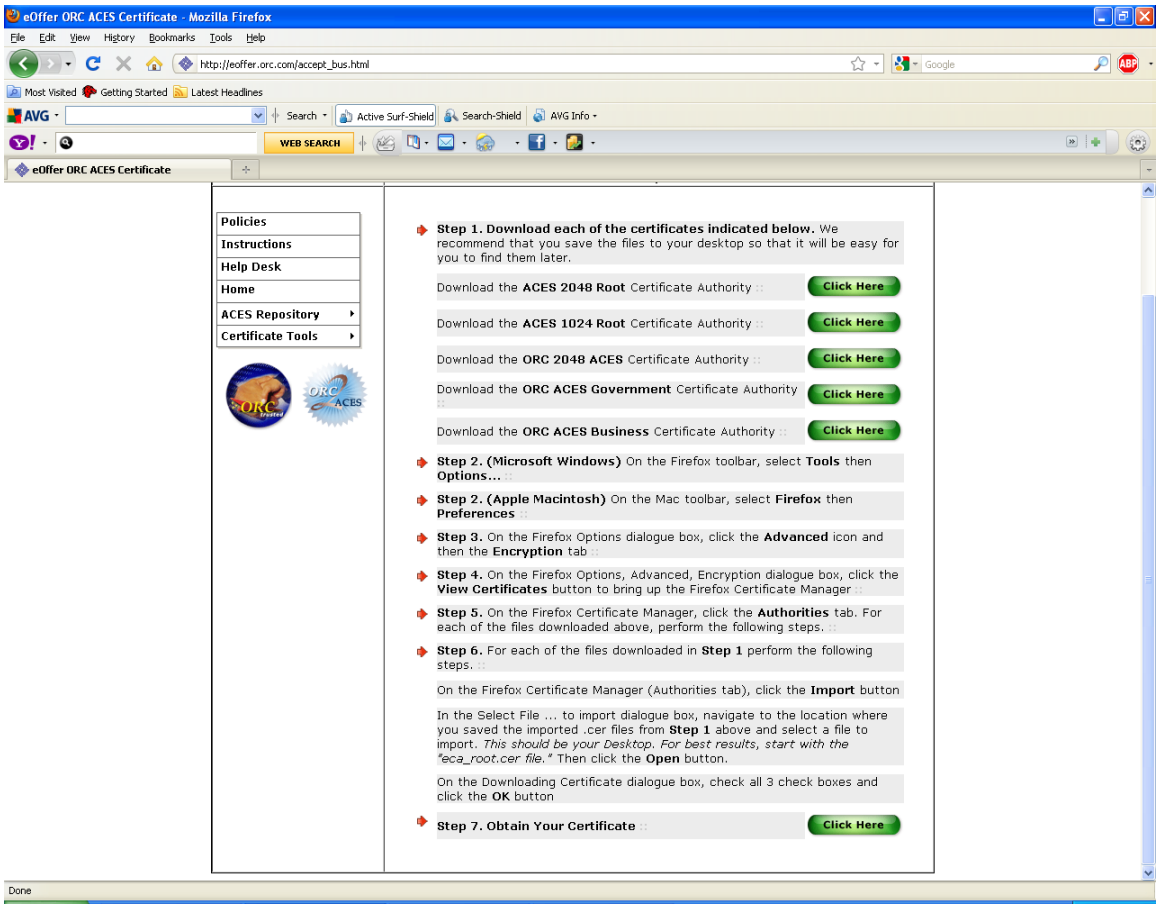
In order to download all of the ACES Root and signing certificate files, you must click the green **Click Here** button next to each certificate.



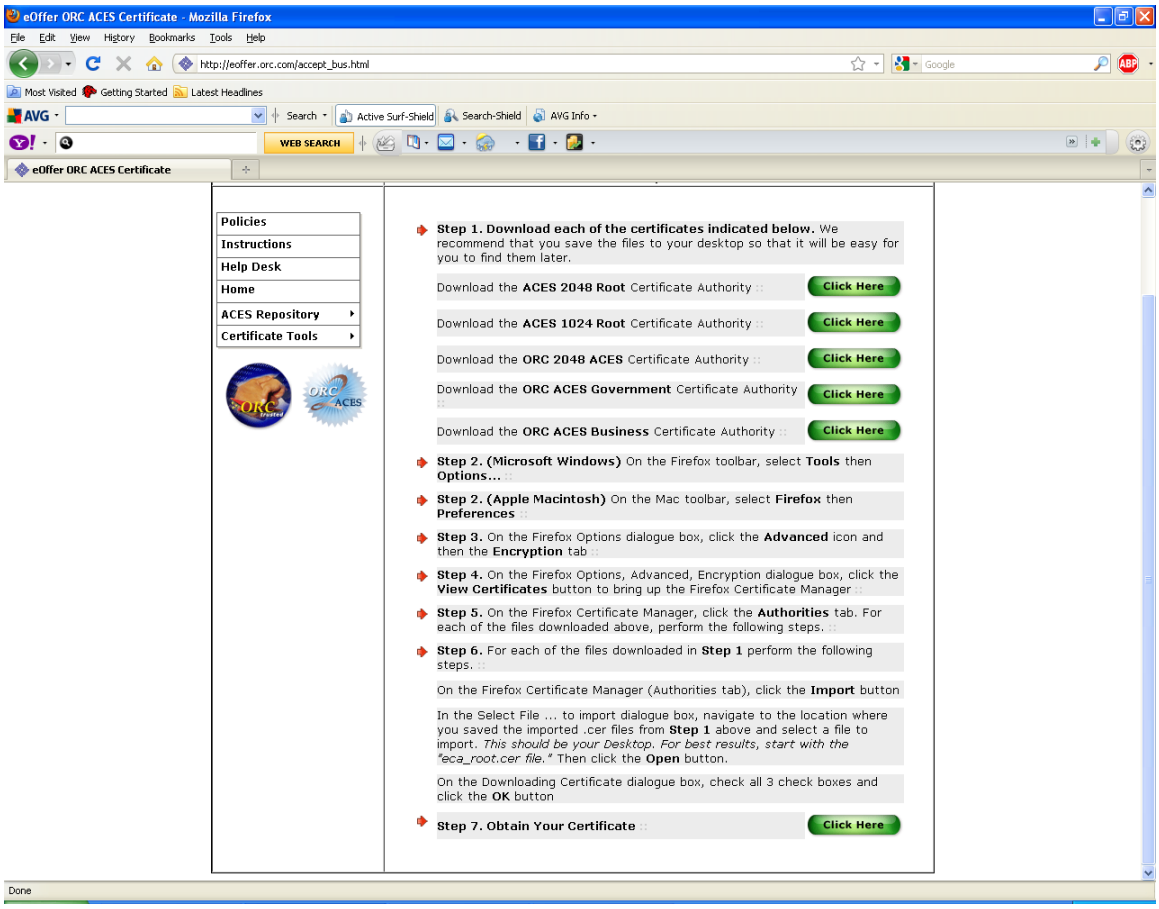
When prompted by Mozilla Firefox about what to do with each .cer file, select **Save File** and click **OK**.



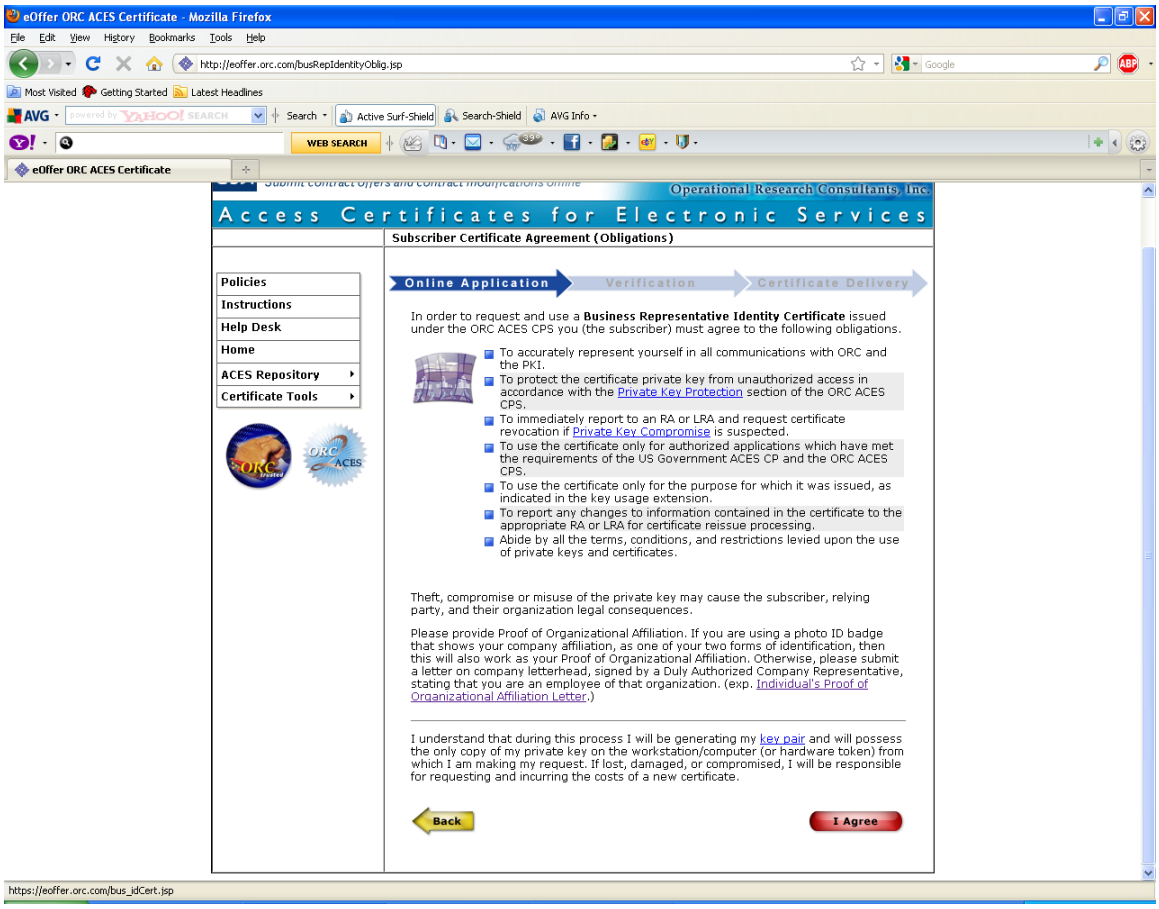
Please follow the instructions from Step 2 to Step 6 in order to install the ACES Root and signing certificate files (ORCRoot.cer, ORC_Government_Root.cer, ORCACES.cer, Government.cer, and Business.cer).



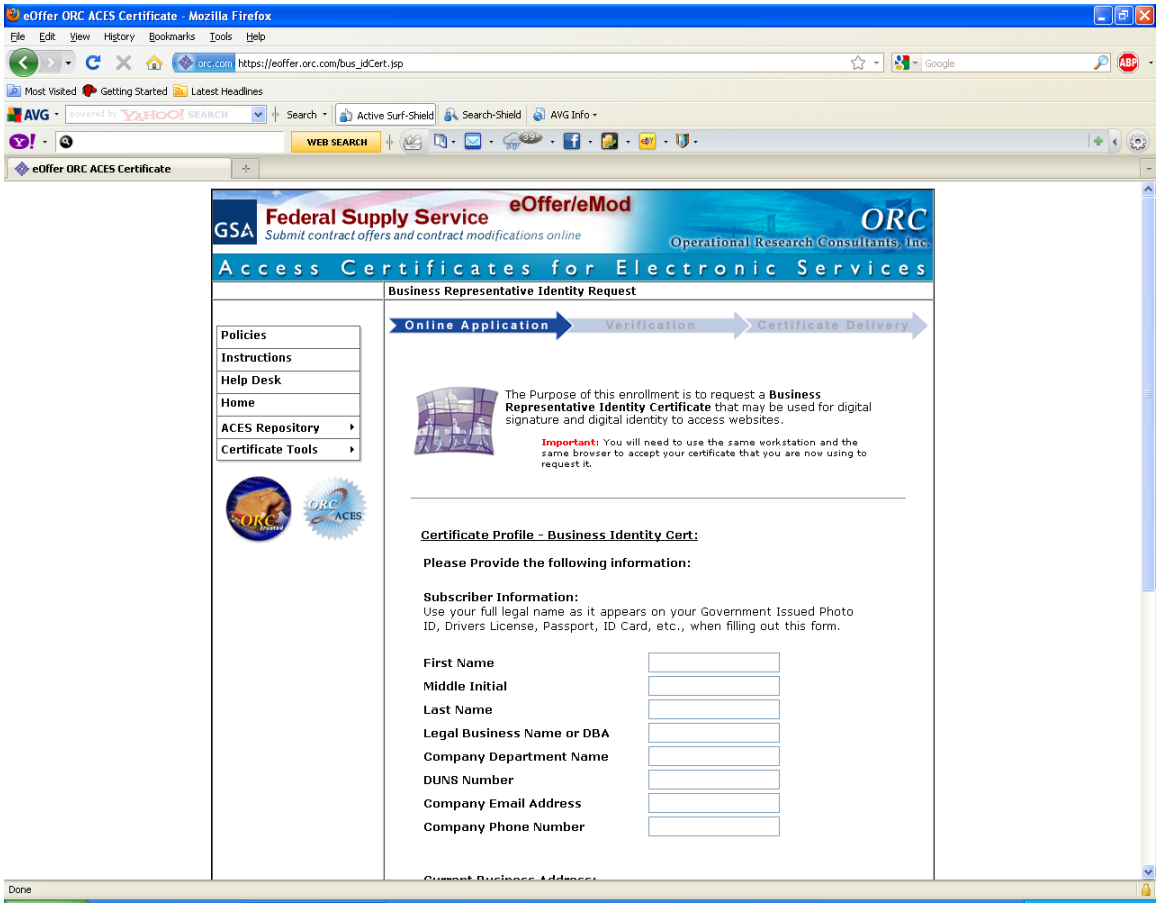
After installing the ACES Root and signing certificate files into Mozilla Firefox, you must click the green button next to Step 7.



Click **I Agree** on the **Subscriber Certificate Agreement (Obligations)** page.



On the next page, you will complete the **Business Representative Identity Certificate Request**. After completing the ACES Business identity certificate online application, you will click **Submit**. If all the information provided (e.g. name and email address) is correct, then you must click **This Is Correct**.

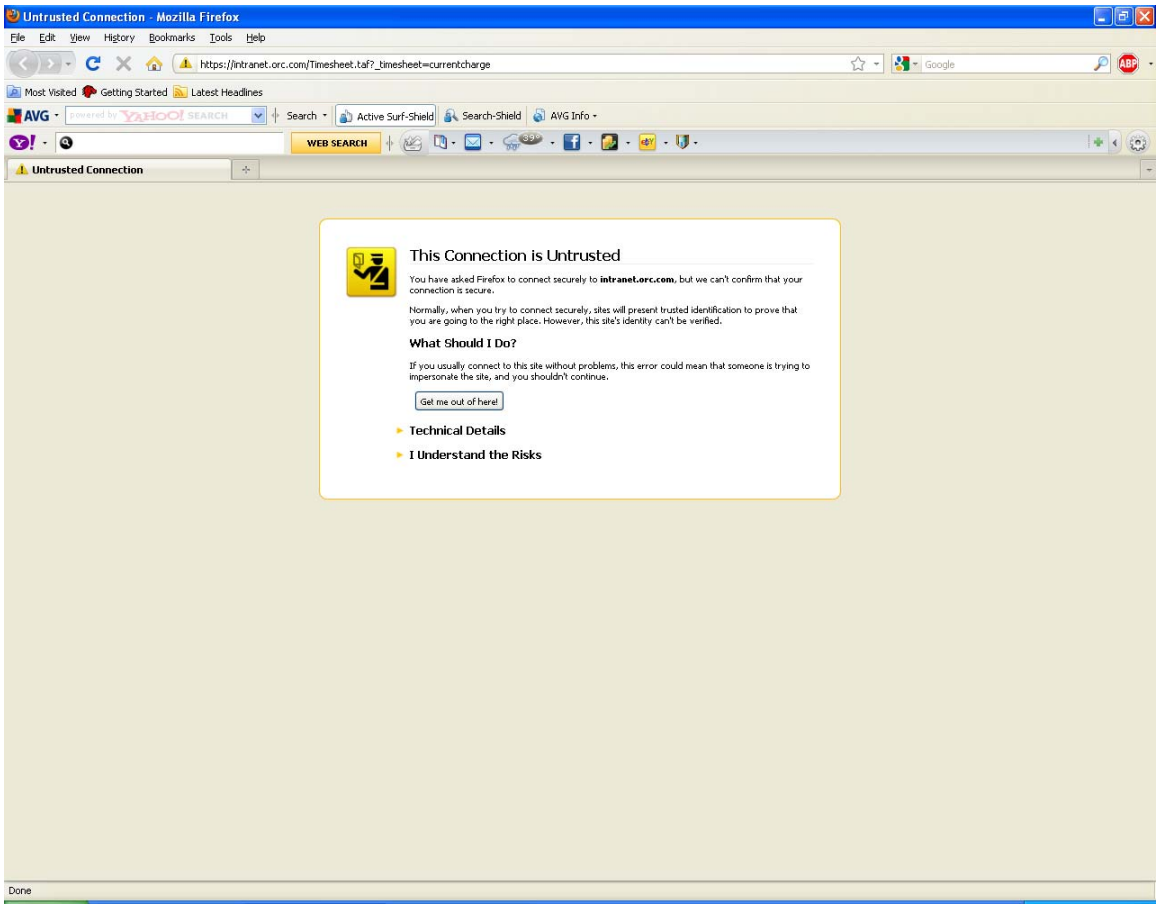


Once you completed the online submission, you must print out the ACES Business identity certificate request form.

After clicking This Is Correct on the ORC ECA online application form, the "**Master Password**" prompt may appear. Subscriber must create their own private key password. The private key password is case-sensitive, and **cannot** be restored or reset by ORC if it is lost or forgotten. The password should be between 8 to 10 characters in length and may include letters and numbers.

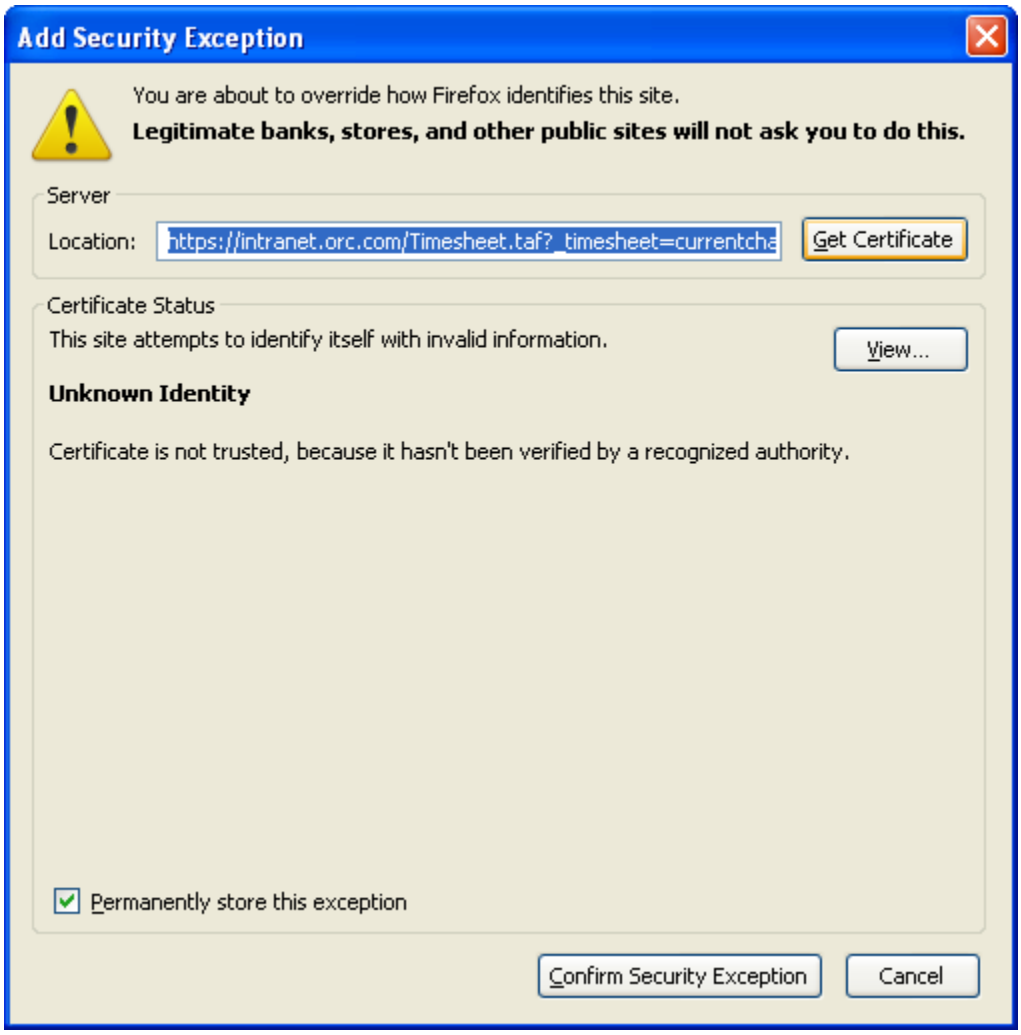
NOTE:
Reminder to any subscribers using Mozilla Firefox who encounter warning message "**This Connection Is Untrusted**"

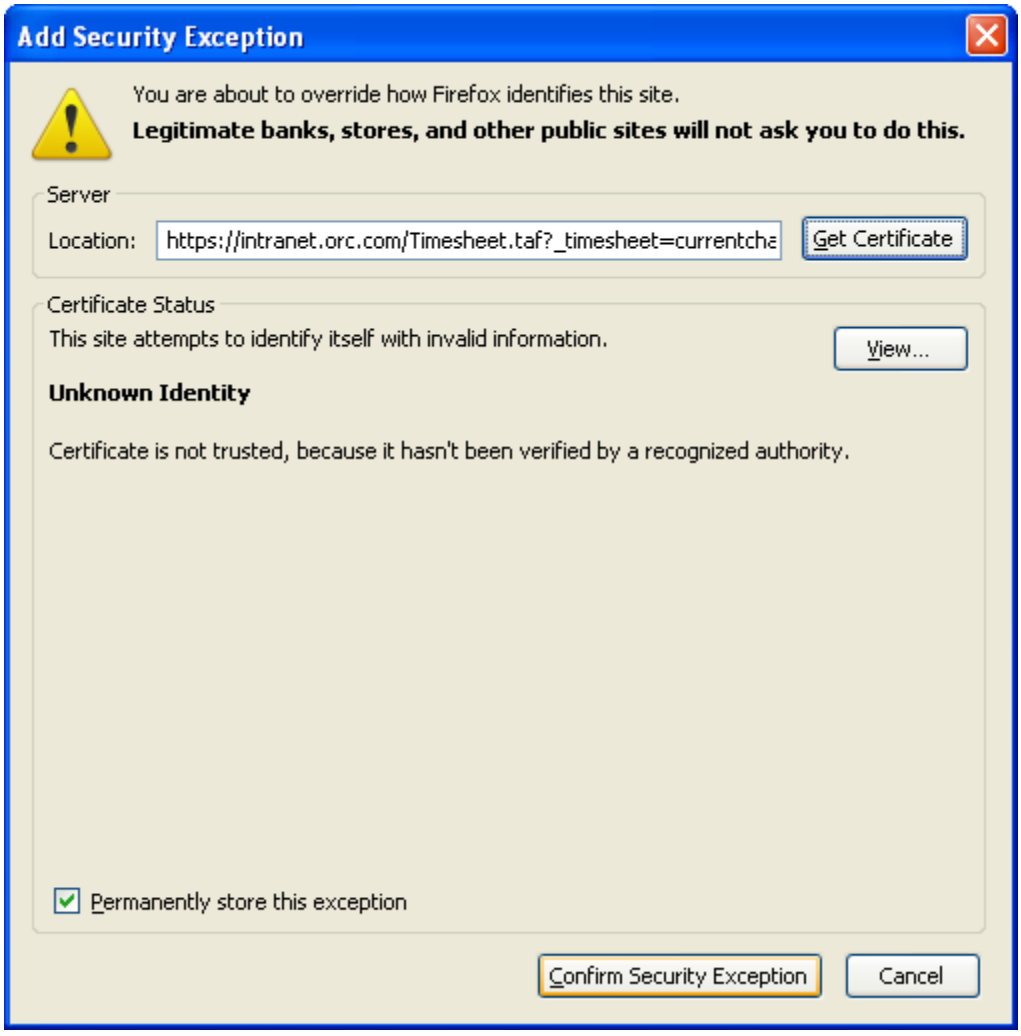
Please disregard the website security warning message "**This Connection Is Untrusted**", which Mozilla Firefox 3 and Mozilla Firefox 3.5 (and above) brings up when encountering an unknown (e.g. untrusted) website security certificate.



Users of Mozilla Firefox 3 can bypass the warning message by clicking "**Or you can add an exception**", then clicking "**Get certificate**", and then clicking "**Confirm Security Exception**".

Users of Mozilla Firefox 3.5 and above can bypass the warning message by clicking "**I understand the risks**", then clicking "**Get certificate**", and then clicking "**Confirm Security Exception**".




Add Security Exception
You are about to override how Firefox identifies this site.
Legitimate banks, stores, and other public sites will not ask you to do this.
Server
Location:
https://intranet.orc.com/Timesheet.taf?_timesheet=currentcha
Get Certificate
Certificate Status
This site attempts to identify itself with invalid information.
View...
Unknown Identity
Certificate is not trusted, because it hasn't been verified by a recognized authority.
Permanently store this exception
Confirm Security Exception
Cancel