

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.

eOffer ORC ACES Certificate - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://eoffer.orc.com/reg_Process_Authentication.html

Most Visited Getting Started Latest Headlines

AVG Search Active Surf-Shield Search-Shield AVG Info

WEB SEARCH

eOffer ORC ACES Certificate

GSA Federal Supply Service eOffer/eMod
Submit contract offers and contract modifications online

ORC
Operational Research Consultants, Inc.

Access Certificates for Electronic Services

Application Process Checklist

There are three main processes for obtaining your ORC ACES Certificates. They are [On-line Application](#), [Identity Verification](#), and [Secure On-line Certificate Delivery](#).

On-line Application

- IMPORTANT:** Each Subscriber must perform the Online Application for themselves. You may NOT make an Online Application for another individual. This is grounds for immediate revocation of your certificate. (And any fees paid will not be returned.) *You must use the same computer, same profile (username), and same browser version when retrieving your certificate that you use for the online application process.*
- By the end of the online application process you will have: trusted the ORC ACES Root and the ORC ACES Intermediate Certification Authority, generated a set of keys for your certificate(s) and assigned a password to protect the private key, and printed a customized, four page, certificate request form for each certificate that you need.
- You must use a computer with a FIPS 140-1/2 Level 1 cryptographic compliant web browser. This includes Internet Explorer 5.5 and above and Firefox 1.5 and above.
You must use the same computer, same profile (username), and same browser version when retrieving your certificate that you use for the online application process.
An important note to if you are using Internet Explorer - Error 1B6 message.
- When applicable, the subscriber's organization will provide a point of contact for verification of any roles or authorizations to be included in the subscriber's certificates, via a signed letterhead or digitally signed e-mail.

Back **Next**

http://eoffer.orc.com/appProcessAuth_bus.html

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 CAs** button in order to download the ACES Root and signing certificate files.



GSA Federal Supply Service eOffer/Mod **ORC**
Submit contract offers and contract modifications online Operational Research Consultants, Inc.

Access Certificates for Electronic Services

Trust the Certificate Authority

[Trust the Certificate Authority](#)

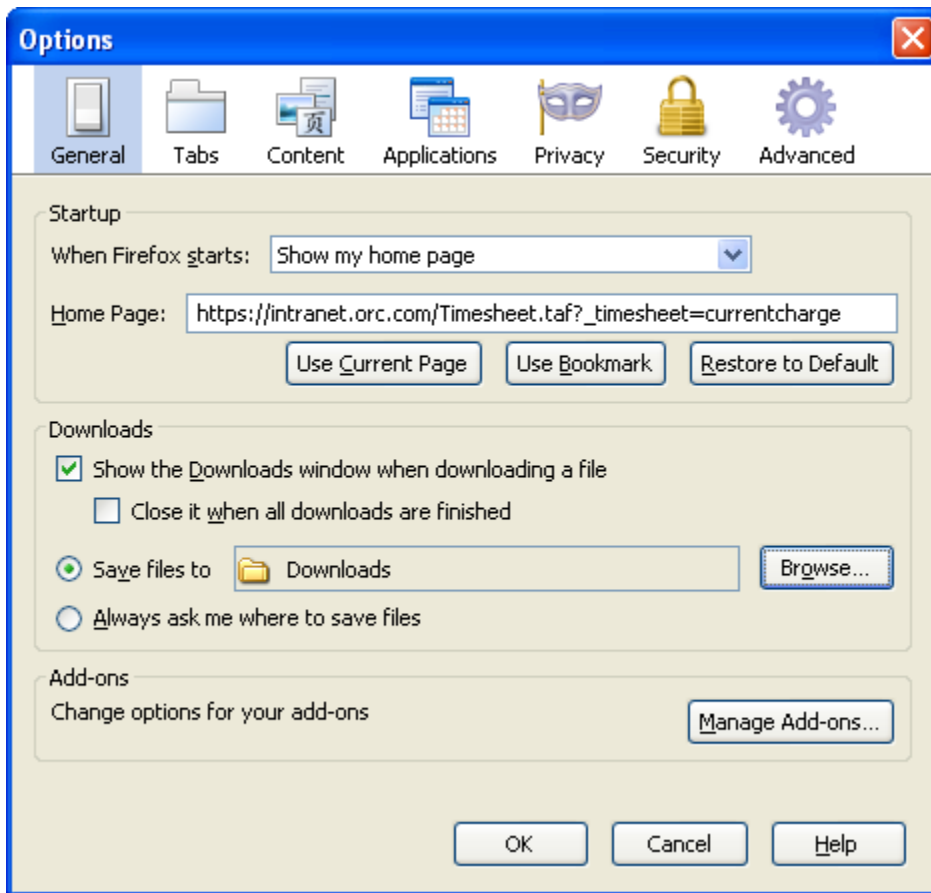
You will need to Trust the ORC ACES Root Certificate Authority. This only needs to be done once (unless there is a notice telling you that an update was made). A browser check will be conducted sending you to the appropriate page.

If you HAVE NOT already trusted the ORC ACES Root Certificate Authority, then please click the button below.	If you HAVE already trusted the ORC ACES Root Certificate Authority, then please click the button below.
Trust CA's	Continue

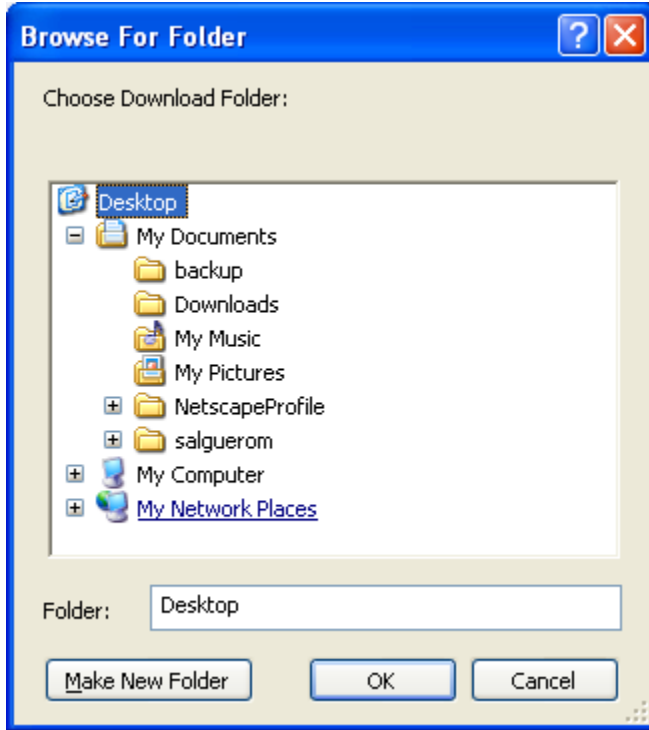
[Back](#)

Policies
Instructions
Help Desk
Home
ACES Repository ▶
Certificate Tools ▶

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.

The screenshot shows a Mozilla Firefox browser window with the address bar displaying http://eoffer.orc.com/accept_bus.html. The page title is "eOffer ORC ACES Certificate".

Sidebar Navigation:

- Policies
- Instructions
- Help Desk
- Home
- ACES Repository
- Certificate Tools

Main Content Area:

Step 1. Download each of the certificates indicated below. We recommend that you save the files to your desktop so that it will be easy for you to find them later.

- Download the **ACES 2048 Root Certificate Authority** :: [Click Here](#)
- Download the **ACES 1024 Root Certificate Authority** :: [Click Here](#)
- Download the **ORC 2048 ACES Certificate Authority** :: [Click Here](#)
- Download the **ORC ACES Government Certificate Authority** :: [Click Here](#)
- Download the **ORC ACES Business Certificate Authority** :: [Click Here](#)

Step 2. (Microsoft Windows) On the Firefox toolbar, select **Tools** then **Options...**

Step 2. (Apple Macintosh) On the Mac toolbar, select **Firefox** then **Preferences**

Step 3. On the Firefox Options dialogue box, click the **Advanced** icon and then the **Encryption** tab

Step 4. On the Firefox Options, Advanced, Encryption dialogue box, click the **View Certificates** button to bring up the Firefox Certificate Manager

Step 5. On the Firefox Certificate Manager, click the **Authorities** tab. For each of the files downloaded above, perform the following steps.

Step 6. For each of the files downloaded in **Step 1** perform the following steps.

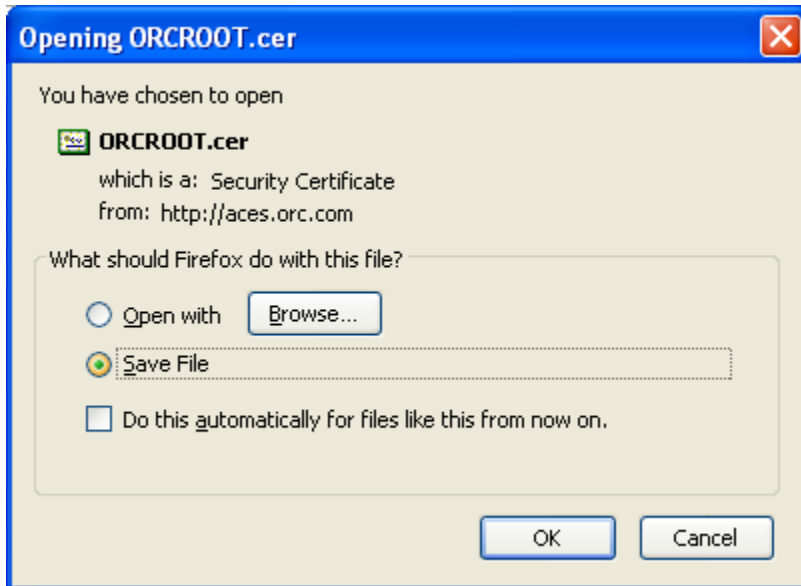
On the Firefox Certificate Manager (Authorities tab), click the **Import** button

In the Select File ... to import dialogue box, navigate to the location where you saved the imported .cer files from **Step 1** above and select a file to import. *This should be your Desktop. For best results, start with the "eca_root.cer" file.* Then click the **Open** button.

On the Downloading Certificate dialogue box, check all 3 check boxes and click the **OK** button

Step 7. Obtain Your Certificate :: [Click Here](#)

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).

eOffer ORC ACES Certificate

File Edit View History Bookmarks Tools Help

http://eoffer.orc.com/accept_bus.html

Most Visited Getting Started Latest Headlines

AVG Search Active Surf-Shield Search-Shield AVG Info

WEB SEARCH

Policies

Instructions

Help Desk

Home

ACES Repository

Certificate Tools

Step 1. Download each of the certificates indicated below. We recommend that you save the files to your desktop so that it will be easy for you to find them later.

Download the **ACES 2048 Root** Certificate Authority :: [Click Here](#)

Download the **ACES 1024 Root** Certificate Authority :: [Click Here](#)

Download the **ORC 2048 ACES** Certificate Authority :: [Click Here](#)

Download the **ORC ACES Government** Certificate Authority :: [Click Here](#)

Download the **ORC ACES Business** Certificate Authority :: [Click Here](#)

Step 2. (Microsoft Windows) On the Firefox toolbar, select **Tools** then **Options...**

Step 2. (Apple Macintosh) On the Mac toolbar, select **Firefox** then **Preferences**

Step 3. On the Firefox Options dialogue box, click the **Advanced** icon and then the **Encryption** tab

Step 4. On the Firefox Options, Advanced, Encryption dialogue box, click the **View Certificates** button to bring up the Firefox Certificate Manager

Step 5. On the Firefox Certificate Manager, click the **Authorities** tab. For each of the files downloaded above, perform the following steps:

Step 6. For each of the files downloaded in **Step 1** perform the following steps:

On the Firefox Certificate Manager (Authorities tab), click the **Import** button

In the Select File ... to import dialogue box, navigate to the location where you saved the imported .cer files from **Step 1** above and select a file to import. *This should be your Desktop. For best results, start with the "eca_root.cer" file.* Then click the **Open** button.

On the Downloading Certificate dialogue box, check all 3 check boxes and click the **OK** button

Step 7. Obtain Your Certificate :: [Click Here](#)

Done

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

The screenshot shows a Mozilla Firefox browser window with the address bar displaying `http://eoffer.orc.com/accept_bus.html`. The page content is as follows:

- Left Sidebar:**
 - Policies
 - Instructions
 - Help Desk
 - Home
 - ACES Repository
 - Certificate Tools
 - Logos for ORC and ACES
- Main Content Area:**
 - Step 1.** Download each of the certificates indicated below. We recommend that you save the files to your desktop so that it will be easy for you to find them later.
 - Download the ACES 2048 Root Certificate Authority :: [Click Here](#)
 - Download the ACES 1024 Root Certificate Authority :: [Click Here](#)
 - Download the ORC 2048 ACES Certificate Authority :: [Click Here](#)
 - Download the ORC ACES Government Certificate Authority :: [Click Here](#)
 - Download the ORC ACES Business Certificate Authority :: [Click Here](#)
 - Step 2. (Microsoft Windows)** On the Firefox toolbar, select **Tools** then **Options...**
 - Step 2. (Apple Macintosh)** On the Mac toolbar, select **Firefox** then **Preferences**
 - Step 3.** On the Firefox Options dialogue box, click the **Advanced** icon and then the **Encryption** tab
 - Step 4.** On the Firefox Options, Advanced, Encryption dialogue box, click the **View Certificates** button to bring up the Firefox Certificate Manager
 - Step 5.** On the Firefox Certificate Manager, click the **Authorities** tab. For each of the files downloaded above, perform the following steps.
 - Step 6.** For each of the files downloaded in **Step 1** perform the following steps:
 - On the Firefox Certificate Manager (Authorities tab), click the **Import** button
 - In the Select File ... to import dialogue box, navigate to the location where you saved the imported .cer files from **Step 1** above and select a file to import. *This should be your Desktop. For best results, start with the "eca_root.cer" file.* Then click the **Open** button.
 - On the Downloading Certificate dialogue box, check all 3 check boxes and click the **OK** button
 - Step 7. Obtain Your Certificate** :: [Click Here](#)

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

The screenshot shows a Mozilla Firefox browser window displaying the website for Operational Research Consultants, Inc. The page title is "Access Certificates for Electronic Services" and the main heading is "Subscriber Certificate Agreement (Obligations)".

On the left side, there is a navigation menu with the following items: Policies, Instructions, Help Desk, Home, ACES Repository, and Certificate Tools. Below the menu are logos for ORC and ACES.

The main content area features a progress bar with three steps: "Online Application" (highlighted), "Verification", and "Certificate Delivery". Below the progress bar, the text states: "In order to request and use a **Business Representative Identity Certificate** issued under the ORC ACES CPS you (the subscriber) must agree to the following obligations."

A list of obligations follows, each preceded by a blue square bullet point:

- To accurately represent yourself in all communications with ORC and the PKI.
- To protect the certificate private key from unauthorized access in accordance with the [Private Key Protection](#) section of the ORC ACES CPS.
- To immediately report to an RA or LRA and request certificate revocation if [Private Key Compromise](#) is suspected.
- To use the certificate only for authorized applications which have met the requirements of the US Government ACES CP and the ORC ACES CPS.
- To use the certificate only for the purpose for which it was issued, as indicated in the key usage extension.
- To report any changes to information contained in the certificate to the appropriate RA or LRA for certificate reissue processing.
- Abide by all the terms, conditions, and restrictions levied upon the use of private keys and certificates.

Below the list, a paragraph states: "Theft, compromise or misuse of the private key may cause the subscriber, relying party, and their organization legal consequences."

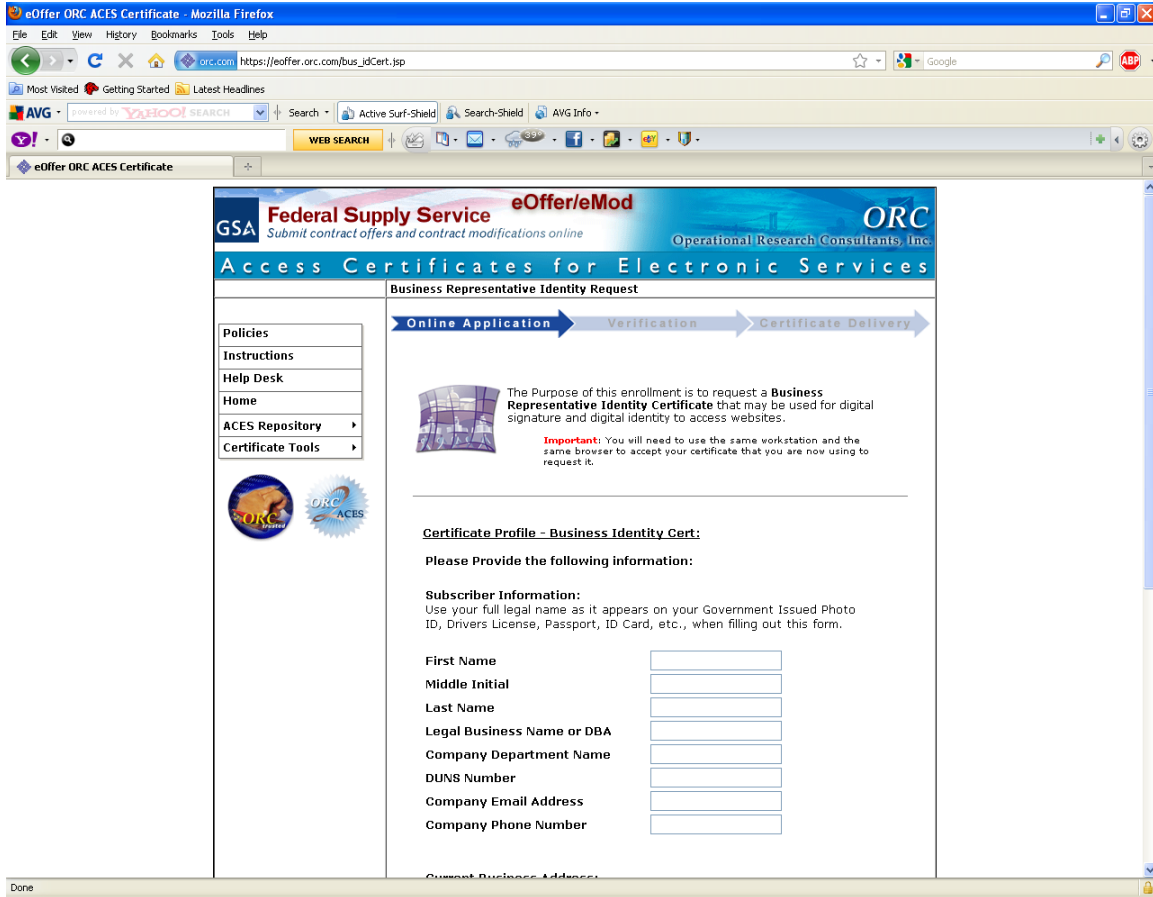
The next paragraph reads: "Please provide Proof of Organizational Affiliation. If you are using a photo ID badge that shows your company affiliation, as one of your two forms of identification, then this will also work as your Proof of Organizational Affiliation. Otherwise, please submit a letter on company letterhead, signed by a Duly Authorized Company Representative, stating that you are an employee of that organization. (exp. [Individual's Proof of Organizational Affiliation Letter](#).)"

A final paragraph states: "I understand that during this process I will be generating my [key pair](#) and will possess the only copy of my private key on the workstation/computer (or hardware token) from which I am making my request. If lost, damaged, or compromised, I will be responsible for requesting and incurring the costs of a new certificate."

At the bottom of the page, there are two buttons: a yellow "Back" button on the left and a red "I Agree" button on the right.

The browser's address bar shows the URL: https://eoffer.orc.com/bus_idCert.jsp

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**.



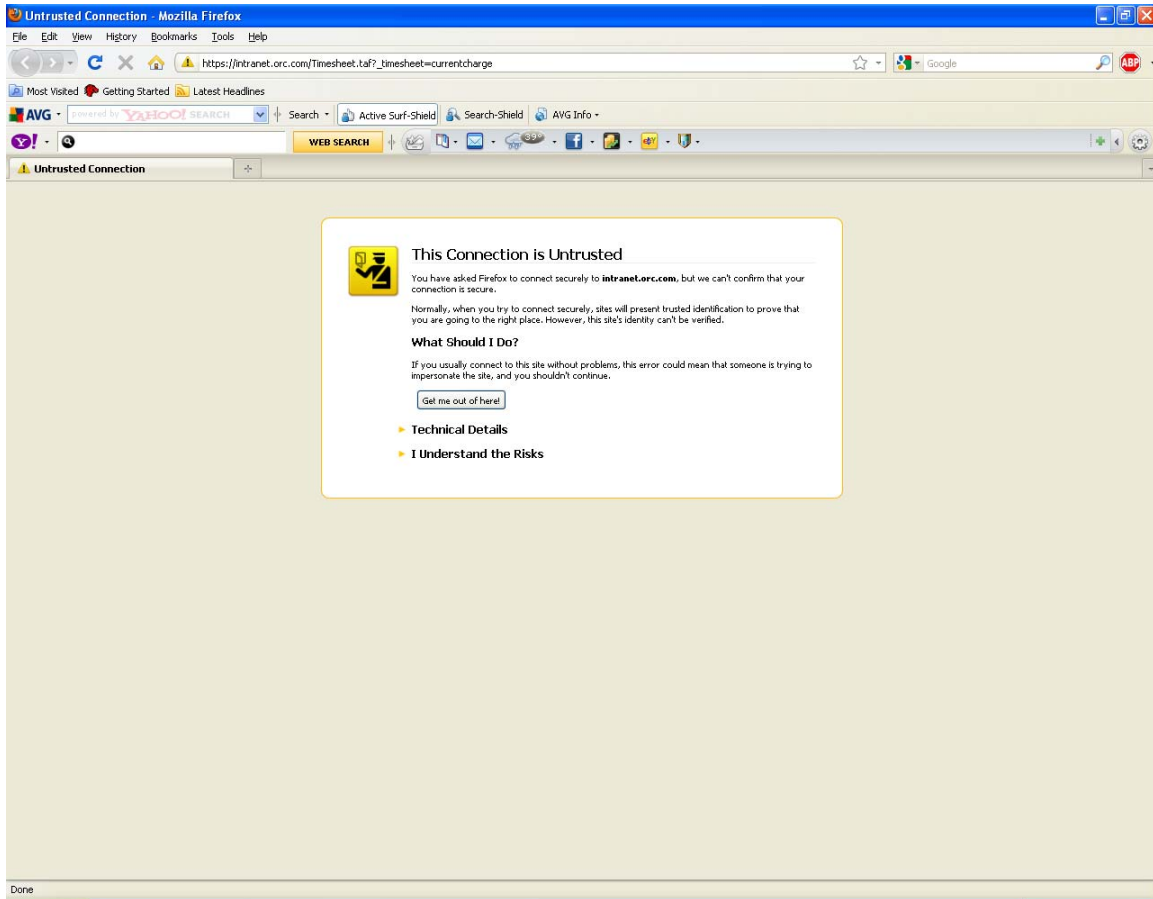
Once you completed the online submission, you must print out the ACES Business identity certificate request form.

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:

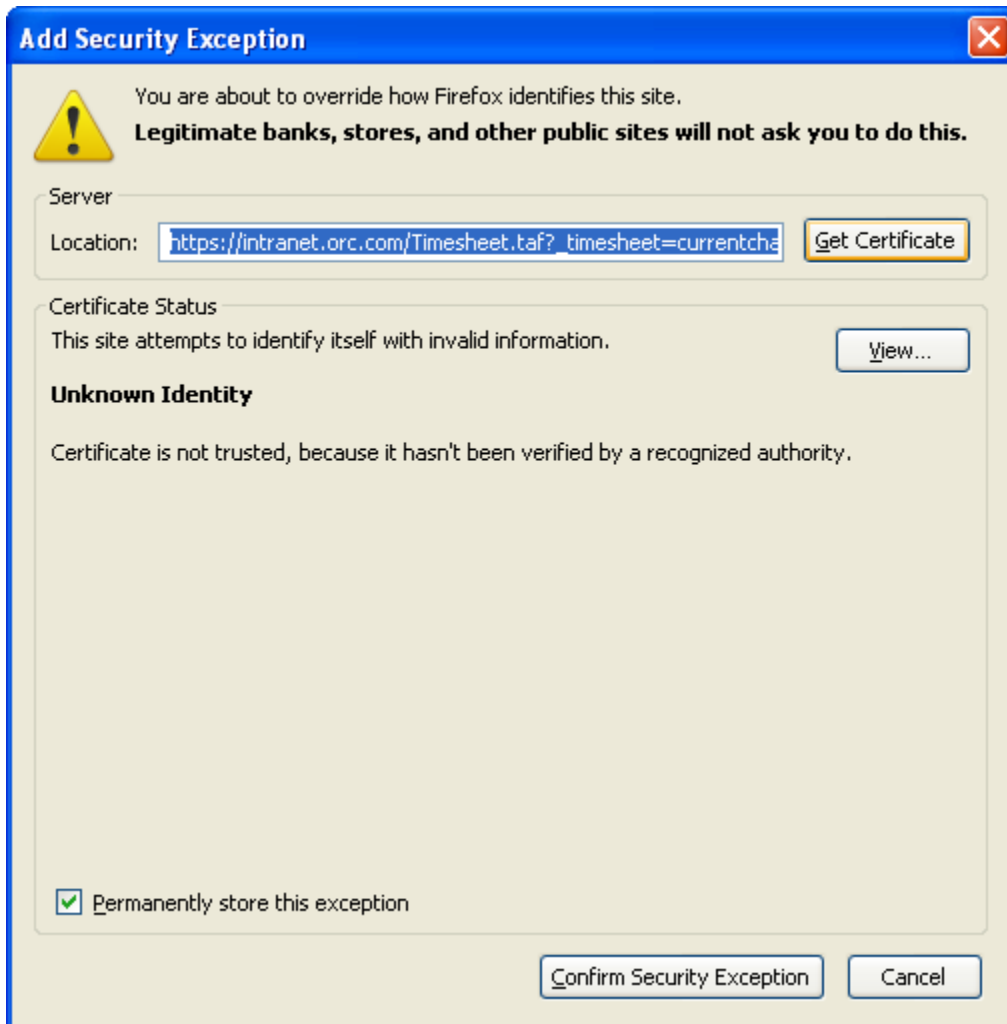
Reminder to any subscribers using Mozilla Firefox who encounter warning message "**This Connection Is Untrusted**"

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:

Certificate Status

This site attempts to identify itself with invalid information.

Unknown Identity

Certificate is not trusted, because it hasn't been verified by a recognized authority.

Permanently store this exception