Subscriber Instructions for ACES Business Identity and Encryption Requests

BEFORE YOU BEGIN: Be sure to use the correct browser

ORC's ACES Business Identity and Encryption Certificates are usable in either Internet Explorer or Mozilla Firefox. However, at this time, you MUST use Mozilla Firefox to generate your certificate request forms. If you want to use your certificates in Internet Explorer, we can provide you instructions for moving the certificate to Internet Explorer after it has been issued.

Please be aware that you may not use Google Chrome or Safari to make your online requests.

When you are ready to begin the certificate request process, use Mozilla Firefox to go to http://aces.orc.com/, then click the blue "order" button next to "ACES Business Representative Certificates".

Step 1: Read the requirements.

- **IMPORTANT:** You must perform the online request for yourself, in your own name. You may NOT make an online request for another individual. This is grounds for immediate revocation of the certificate, and any fees paid will not be returned.
- **GSA-specific note:** You should use your own email address (and it should match your address on file with GSA). Also note that we have been informed that GSA has a policy of "one user per email address". If multiple individuals at your company intend to become ACES certificate holders, each person should use a different email address.
- The ACES Certificate Policy requires that we issue your name in a specific format "Firstname MI Lastname (Suffix)". This information must match the information on your current, government-issued photo ID that you present to the Notary Public/Registration Authority. **GSA-specific note**: If your name is currently listed in GSA's records differently than how it is issued on your certificate, you must have your GSA Contracting Officer change the entry in GSA's records. Your certificate can ONLY be issued using your legal name, in the format specified above, and will NOT be issued in a different way to match your GSA contract.
- A workstation with a FIPS 140-1/2 Level 1 cryptographic compliant web browser is required. This includes Internet Explorer 5.5 and above and Firefox 1.5 and above. **At this time, requests may only be made through Firefox**. Do not attempt to make your request through other browsers, such as Internet Explorer, Google Chrome or Safari. After your certificate has been issued and you have imported and backed it up through Firefox, you may use your backup file to import the certificate into Internet Explorer for use in that browser.
- The computer, web browser, and network profile that you are now using must also be used to import your certificate after ORC issues it.
- The ACES Certificate Policy requires all Subscribers to protect their certificate private keys with a password or PIN. During the online request process you will have an opportunity to assign a password to protect the certificate private key. ORC will not know this password; it is not sent out from your computer. If you forget your certificate password, you may be required to purchase a new certificate.

Step 2: Gather the required documents.

To verify your identity for the digital certificate request, please gather the following documents:

1. **Two forms of photo identification** (One must be from the primary list below. The second may come from either list, but MUST be from a different issuing agency from the first photo ID.)

Primary Photo ID	Secondary Photo ID
Current photo ID issued by a federal, state, or local government Examples- This list is not exhaustive. You may use any current photo ID issued by a federal state, or local government. ▪ Current, valid passport (U.S. or foreign) ▪ Current, valid driver's license (U.S. or foreign) ▪ Government-issued photo identity card or badge (U.S. or foreign) ▪ U.S. DOD CAC Card	**Non-Exhaustive List of Examples:** ▪ Valid *or expired* passport (U.S. or foreign) ▪ Valid *or expired* driver's license (U.S. or foreign) ▪ Government-issued photo identity card or badge (U.S. or foreign) ▪ U.S. DOD CAC Card ▪ Student photo ID ▪ Official photo identity card or badge from your company or institution ▪ Credit card (with photo) ▪ An ID that does not show both your photo and your name **will not** be accepted as one of your two photo IDs. (e.g. Social Security card, voter registration, etc.)

2. **One of the following Proofs of Organizational Affiliation**
   - A current, company-issued photo ID with company name, employee name, and employee photo.
   - A letter on company letterhead, signed by a Duly Authorized Company Representative, stating that you are an employee of that organization. A proof of affiliation letter is not a substitute for one of the above required photo IDs. (Download example)

Step 3: Trust the CAs.

You will need to trust the ACES Certificate Authorities. This only needs to be done once per browser per computer. A browser check will be conducted, sending you to the appropriate page.

If you have already trusted the ACES Certificate Authorities, then you may continue Step 4: Request your ACES Certificates.

If you have not previously trusted the ACES Certificate Authorities, follow the instructions on the page to do so. Then, continue to Step 4: Request your ACES Certificates

Step 4: Fill out and print the online request forms.

Fill out the online request form and follow the on-screen instructions to generate and print your request forms. At the end of the process, you will have a single, two-page request form used for requesting the identity certificate and, if you opted to request one, the encryption certificate as well.

Step 5: Make a backup copy of your enrollment keys.

You have generated certificate requests and key pairs.

It is strongly recommended that you back-up your Enrollment Key Pairs. This will serve to verify that keys were generated and that you are in possession of the passwords assigned to protect these key pairs. Additionally, if you put the back-up files on external media (CD, thumb drive, etc.), this will mitigate the risk of technical problems destroying your certificates.

You can find instructions for backing up your enrollment keys here:
http://eca.orc.com/wp-content/uploads/ECA_Docs/Backup_Copy_Firefox_Cert_Store.pdf

Once you have successfully made backup files of your Enrollment keys, you can take your request forms to the Notary.

Step 6: Have the printed request forms (with the required documents) notarized. Mail the documents to ORC, and await receipt of your digital certificates.

After you complete the online request, you must take your request forms and the required identity documentation to a Trusted Agent for identity verification. Your options for a Trusted Agent depend on your location. Choose the description below that applies to you.

I am located in the US

You may visit any of the following to have your identity verification performed:

- a notary public
- an ORC Registration Authority (RA) at either our Fairfax, Virginia or our Chesapeake, Virginia office.
- an authorized Local Registration Authority (LRA) at your company

I am located in Australia, Canada, Great Britain, or New Zealand

You may visit one of the following to have your identity verification performed:

- a notary public
- a US Consular Notary at a US Embassy or Consular office

I am located in a country other than those shown above

You **must** visit the following to have your identity verification performed:

- a US Consular Notary at a US Embassy or Consular office

After you have your requests notarized

After you have had the identity verification performed by one of the above Trusted Agents, you must send the original, notarized request forms (no photocopies) to our Fairfax, Virginia office by the carrier of your choice (FedEx, UPS, USPS, etc). Our address is located on the first page of the request form. Request forms may NOT be submitted to us by fax or email. You must also include copies of the required identity documentation as detailed on the verification page.

We will process your request within 3-5 business days of its arrival at our Fairfax, Virginia office. Within that time frame, you will receive an email that either:

- Informs you of any problems with the request and explains how to rectify the problems; OR
- Informs you that your certificate has been issued and provides complete instructions on how to import, test, and create a backup copy of your certificate.

Our emails may be mistaken for spam by your company’s spam filter. Please watch your spam/junk folder for any messages from an orc.com email address. If you haven’t received an email from us about your certificate request within 5 business days of its arrival at our office, you can inquire about its status by emailing our help desk at aceshelp@orc.com. (You may wish to whitelist email from the ORC.COM domain.)

Remember that when importing your certificate, you must use the same computer, network profile (log on), and web browser that you used to make the request. Please refrain from all updates of browser and operating system until your certificates have been successfully imported.