In order for an application (like Internet Explorer or Outlook) to make use of a certificate without sending up a host or warning messages, the application must be told to ‘trust’ the certificate. The most efficient way to tell an application that certificates are trusted is to trust Certificate Authorities. A Certificate Authority (CA) is an entity that issues certificates. By trusting an entire CA, you trust all certificates issued by that CA. Microsoft comes with many commercial CAs ‘pre-trusted’ before you ever turned the computer on. But the CAs authorized by the Federal Government do not (as yet) come pre-trusted.

These instructions will tell you how to Trust the ORC ECA Certificate Authority, so that Microsoft applications will not give you warnings about your certificates (or any other certificates issued by the ORC ECA CA).

Note: If you have ECA certificates then you are trying to communicate with the US Department of Defense (US DoD). The US DoD has two Certificate Authority programs; the DoD PKI and the DoD External Certification Authority (ECA) PKI. The DoD PKI consists of the US DoD issuing certificates internally to US DoD end entities (like DoD employees and DoD web sites). The ECA PKI consists of vendors that are authorized by the US DoD to issue certificates to end entities outside of the US DoD that need to communicate with the DoD. You probably need to trust both the DoD PKI and ECA PKI. If so, look at our instructions for Trusting the DoD PKIs; if you perform those instructions, then you will not need to perform the instructions below.

*These instructions and associated screen captures were created with Internet Explorer 11 running on a Windows 10 operating system. Variations in versions of Internet Explorer and the Windows Operating system will result in some variation of alert boxes and screen images. For the most part, the process and individual steps are the same across Windows platforms. (You might see a dialog box prompting you to ‘allow’ access on a Windows Windows 7/8 computer; just click the buttons that seem to move the process forward.)*
1. Start Internet Explorer. In the address bar, go to: [https://eca.orc.com/order/trust-cas/trust-page-for-internet-explorer/](https://eca.orc.com/order/trust-cas/trust-page-for-internet-explorer/)

   To trust the ORC ECA manually (rather than using InstallRoot as indicated above) follow the instructions below.

   Print and keep this page for reference. Upon clicking the links for Step 1 through Step 7 below your browser will prompt you to open the certificate prior to installing it. Follow the sequence below as you install the ECA Root and ORC ECA Certificates.

   - Step A. Trust the ECA Root CA 4 Certificate Authority
   - Step B. Trust the ECA Root 2 Certificate Authority
   - Step C. Trust the ECA 6 Certificate Authority
   - Step D. Trust the ECA 7 Certificate Authority
   - Step E. Trust the ORC ECA CA SWS Certificate Authority
   - Step F. Trust the ORC ECA CA HWS Certificate Authority

2. Click on Step A Trust the ECA Root CA 4 Certificate Authority. *(Always try to trust the Root Certificate of any CA first.)*

3. When asked if you want to open this file now, click the **Open** button. If asked additionally click on the **Allow** button.
4. On the Certificate dialog box, click the **Install Certificate**… button.
Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: ECA Root CA 4

Issued by: ECA Root CA 4

Valid from 03/20/2012 to 12/30/2029

This is what we are fixing

Install Certificate...
5. When the Certificate Import Wizard pops up, click on the Next > button.

6. On the Certificate Store dialog, select “Place all certificates in the following store” and then click the Browse... button.
7. Select the **Trusted Root Certification Authorities** folder and click the **OK** button.
8. Back on the Certificate Store dialog, click the **Next >** button.

9. On the Completing the Certificate Import Wizard, click on the **Finish** button.
Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

<table>
<thead>
<tr>
<th>Certificate Store Selected by User</th>
<th>Trusted Root Certification Authorities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content</td>
<td>Certificate</td>
</tr>
</tbody>
</table>
10. In the Security Warning dialog box, click the Yes button.

11. At “The import was successful, click the OK button.

12. On the Certificate dialog box, click the OK button. The Certificate dialog box will disappear.
13. Back on the web page Click on Step B Trust the ORC ECA SW3 Certificate Authority. *(This is a specific ORC CA server that issues Medium Assurance or browser-based certificates.)*
14. When asked if you want to open this file now, click the **Open** button. If asked additionally click on the **Allow** button.

![Image of certificate dialog box with 'Open' button highlighted]

15. On the Certificate dialog box, click the **Install Certificate...** button.
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

**Issued to:** ECA Root CA 2

**Issued by:** ECA Root CA 2

**Valid from** 04/04/2008 **to** 03/30/2028

This is what we are fixing

Install Certificate...
When the Certificate Import Wizard pops up, click on the **Next >** button.

---

**Welcome to the Certificate Import Wizard**

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

**Store Location**

- [ ] **Current User**
- [ ] **Local Machine**

To continue, click Next.
17. On the Certificate Store dialog, select “Place all certificates in the following store” and then click the **Browse…** button.

18. Select the **Trusted Root Certification Authorities** folder and click the **OK** button.
20. On the Completing the Certificate Import Wizard, click on the **Finish** button.
21. In the Security Warning dialog box, click the **Yes** button.
22. At “The import was successful, click the OK button.

23. On the Certificate dialog box, click the OK button. The Certificate dialog box will disappear.
24. Click on Step C Trust the ECA 6 Certificate Authority

25. When asked if you want to open this file now, click the Open button. If asked additionally click on the Allow button.
Screen 1: Click Open in the “File Download” window. 

Note: If the certificate will not open, select save, and open it from your desktop.

Internet Explorer Security

A website wants to open web content using this program on your computer.

This program will open outside of Protected mode. Internet Explorer's Protected mode helps protect your computer. If you do not trust this website, do not open this program.

Name: Crypto Shell Extensions
Publisher: Microsoft Windows

Do not show me the warning for this program again

Allow | Don't allow
26. On the Certificate dialog box, click the **Install Certificate** button.
27. When the Certificate Import Wizard pops up, click on the **Next >** button.

28. On the Certificate Store dialog, select “Place all certificates in the following store” and then click the **Browse...** button.
29. Select the Intermediate Certification Authorities folder and click the OK button.
30. Back on the Certificate Import Wizard, click the **Next >** button.

31. On the Completing the Certificate Import Wizard, click on the **Finish** button.
32. At “The import was successful, click the OK button.

33. On the Certificate dialog box, click the OK button. The Certificate dialog box will disappear.
34. Click on Step D Trust the ECA 7 Certificate Authority

35. When asked if you want to open this file now, click the Open button. If asked additionally click on the Allow button.
Screen 1: Click Open in the "File Download" window.

**NOTE:** If the certificate will not open, select save, and open it from your desktop.

Do you want to open a file from ecrow.com?
- Open
- Save
- Cancel

Internet Explorer Security

A website wants to open web content using this program on your computer

This program will open outside of Protected mode. Internet Explorer’s Protected mode helps protect your computer. If you do not trust this website, do not open this program.

Name: **Crypto Shell Extensions**
Publisher: **Microsoft Windows**

- [ ] Do not show me the warning for this program again

[Allow] [Don’t allow]
36. On the Certificate dialog box, click the **Install Certificate...** button.
37. When the Certificate Import Wizard pops up, click on the **Next** button.

38. On the Certificate Store dialog, select “Place all certificates in the following store” and then click the **Browse**... button.
39. Select the **Intermediate Certification Authorities** folder and click the **OK** button.
40. Back on the Certificate Import Wizard, click the **Next >** button.

41. On the Completing the Certificate Import Wizard, click on the **Finish** button.
42. At “The import was successful, click the OK button.

43. On the Certificate dialog box, click the OK button. The Certificate dialog box will disappear.
44. Click on Step E Trust the SW5 Certificate Authority

45. When asked if you want to open this file now, click the **Open** button. If asked additionally click on the **Allow** button.
Screen 6: Return to the "Certificate" window. Click OK.

---

Step C. Trust the ECA 6 Certificate Authority

Step D. Trust the ECA 7 Certificate Authority

Step E. Trust the ORC ECA CA SWS Certificate Authority

Step F. Trust the ORC ECA CA HWS Certificate Authority

Screen 1. Click Open in the "File Download" window.

NOTE: If the certificate will not open, select save, and open it from your desktop.

Do you want to open or save [ecacerts.exe] (1.08 KB) from [www.wux.com]? Open Save Cancel

Internet Explorer Security

A website wants to open web content using this program on your computer

This program will open outside of Protected mode. Internet Explorer's Protected mode helps protect your computer. If you do not trust this website, do not open this program.

Name: Crypto Shell Extensions
Publisher: Microsoft Windows

Do not show me the warning for this program again

Allow Don't allow
46. On the Certificate dialog box, click the **Install Certificate...** button.
47. When the Certificate Import Wizard pops up, click on the **Next >** button.

48. On the Certificate Store dialog, select “Place all certificates in the following store” and then click the **Browse...** button.
49. Select the **Intermediate Certification Authorities** folder and click the **OK** button.
50. Back on the Certificate Import Wizard, click the **Next** button.

51. On the Completing the Certificate Import Wizard, click on the **Finish** button.
52. At “The import was successful, click the OK button.

53. On the Certificate dialog box, click the OK button. The Certificate dialog box will disappear.
54. Click on Step F Trust the HW5 Certificate Authority

55. When asked if you want to open this file now, click the Open button. If asked additionally click on the Allow button.
Screen 6: Return to the "Certificate" window: Click OK

---

Step C. Trust the ECA 6 Certificate Authority

Step D. Trust the ECA 7 Certificate Authority

Step E. Trust the ORC ECA CA SWS Certificate Authority

Step F. Trust the ORC ECA CA HWS Certificate Authority

Screen 1: Click Open in the "File Download" window.

**NOTE:** If the certificate will not open, select save, and open it from your desktop.

---

Internet Explorer Security

A website wants to open web content using this program on your computer

This program will open outside of Protected mode. Internet Explorer's Protected mode helps protect your computer. If you do not trust this website, do not open this program.

Name: Crypto Shell Extensions

Publisher: Microsoft Windows

☐ Do not show me the warning for this program again

[Allow] [Don't allow]
56. On the Certificate dialog box, click the **Install Certificate**... button.
57. When the Certificate Import Wizard pops up, click on the **Next >** button.

58. On the Certificate Store dialog, select “Place all certificates in the following store” and then click the **Browse...** button.
59. Select the **Intermediate Certification Authorities** folder and click the **OK** button.
60. Back on the Certificate Import Wizard, click the **Next >** button.

61. On the Completing the Certificate Import Wizard, click on the **Finish** button.
62. At “The import was successful, click the OK button.

63. On the Certificate dialog box, click the OK button. The Certificate dialog box will disappear.
Certificate Information

This certificate is intended for the following purpose(s):
- 2.16.840.1.101.3.2.1.12.1
- 2.16.840.1.101.3.2.1.12.2
- 2.16.840.1.101.3.2.1.12.3
- All application policies

Issued to: ORC ECA HW 5

Issued by: ECA Root CA 2

Valid from 05/19/2014 to 05/18/2020

OK