# ODOT'S EXTERNAL PARTNERS SIGNATURES VERIFICATION GUIDE

**ODOT External Partners**

If you receive a project document with ODOT digital signatures, you need to ensure that you establish trust with ODOT's root certificate. ODOT currently stored their root certificate in the Window's Certificate library. You may need to configure Adobe products to use the Windows Certificate library. Follow the steps below to trust ODOT's root certificate.

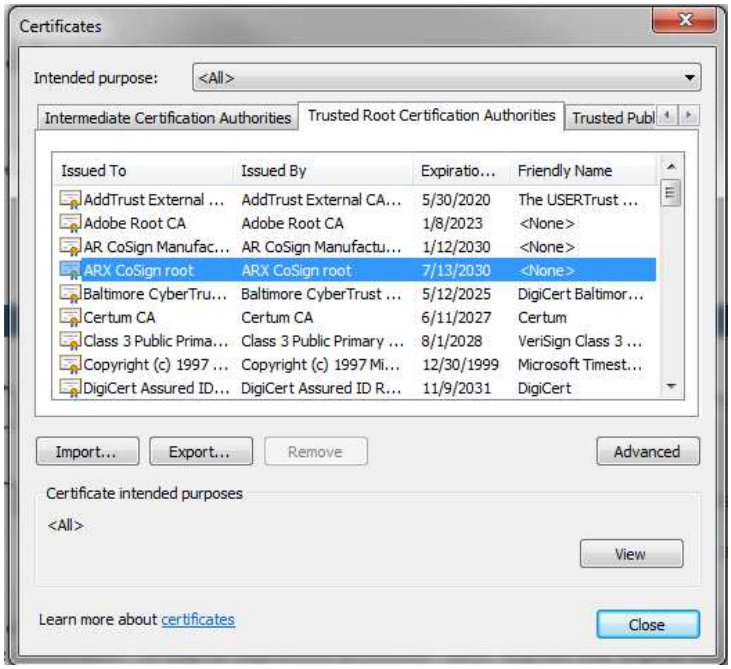
1. Download ODOT's Setup Verifier executable files accessible from the following link

   http://www.oregon.gov/ODOT/ETA/Documents_ETA/SetupVerifier.zip

   http://www.oregon.gov/ODOT/ETA/Documents_ETA/SetupVerifier_Office.zip

2. Run the executable files. This should install the root certificate and enable Adobe product to validate the digital signatures.
3. Verify a trust relationship has been established through the computer's Internet Options setting by opening Internet Explorer and navigating to Internet Options > Content tab > Certificates > Trusted Root Certificate Authorities.

   ARX CoSign root should be listed under Trusted Root Certification Authorities




4. Validate the trust has been established on the digitally signed documents.
   a. When you open the Microsoft Word document, you should see a green checkmark next to the digital signature.
   b. When you open an Adobe file, you should see a message near the top of the file indicating that the file is signed and all signatures are valid.
5. If trust has not been established, the yellow exclamation or a warning or a message stating no trust established for the digital signatures should be displayed.
   a. Try again.

   b. Contact your ODOT Representative.
6. If you are working with a digitally signed pdf and having Trust issues, you can manually enable the Adobe to use the Windows Certificate Library.
   a. Open the Preferences dialog box.
   b. Under Categories, select Signatures.
   c. For Identities & Trusted Certificates, click More…
   d. Select Trusted Certificates on the left.
   e. Select a certificate from the list, and click Edit Trust.
   f. In the Trust tab, select any of the following items to trust this certificate: Use This Certificate As A Trusted Root
   g. A root certificate is the originating authority in a chain of certificate authorities that issued the certificate. By trusting the root certificate, you trust all certificates issued by that certificate authority.

If you receive a document from ODOT requesting your digital signature, follow your contract requirements for digital signatures. Use your Digital Signature software process.

**ODOT Employees**

When you receive a document with a digital signature from an ODOT External partner, you must verify:

1. The digital signature is valid.
2. The certificate associated with the digital signature is current (not expired)
3. The signing person or organization, known as the publisher, is trusted.
4. The certificate associated with the digital signature is issued to the signing publisher by a reputable certificate authority (CA).

Follow the process outlined below.

1. Open the document in the native format.
2. Do the signatures indicate validation, such as a Green checkmark or a Ribbon?
3. Right click on signature to open. Validate that the signature shows a third party CA, not self-signed.
4. If third party still has Trust issues, then root certificate is missing from the Certificate Library. To add a root certificate to Certificate Library, contact ODOT Help Desk.
5. As a last resort, after validating the signed content with the expected sender, manually trust their individual signature.