DoD Public Key Enablement (PKE) Quick Reference Guide

Verifying Digital Signatures on DoD PKE Tools

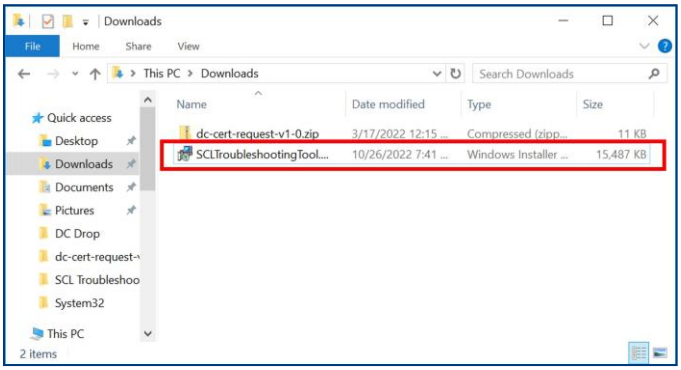
Contact: dodpke@mail.mil
URL: https://www.cyber.mil/pki-pke

Enabling PKI Technology for DoD Users

Before proceeding with any DoD PKE tool installation, verify the installer package has been digitally signed by the DoD PKE team. Follow these steps to quickly verify the digital signature on executable installer files (.exe and .msi).

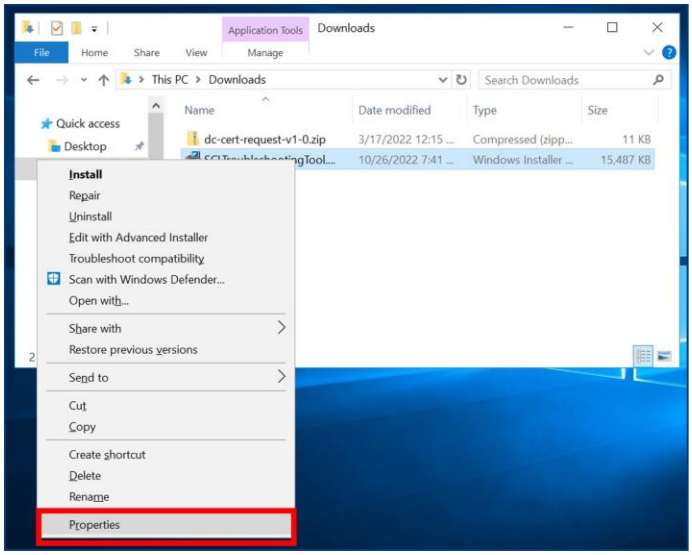
Step 1

In Windows Explorer, navigate to the directory containing the installer package.



Step 2

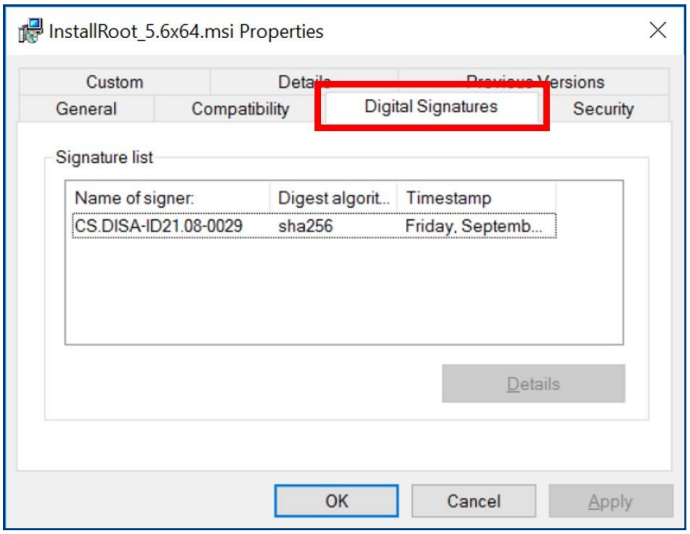
Right-click the installer and select **Properties** from the pop-up menu to open the **Properties** window.



Continued on page 2

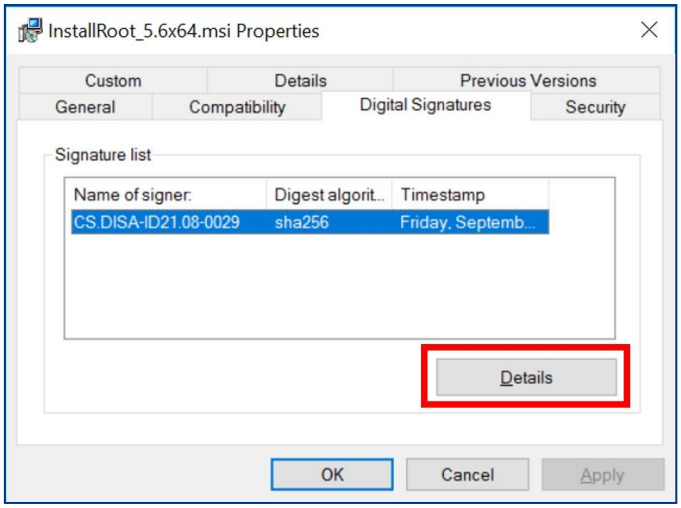
Step 3

Select the **Digital Signatures** tab.



Step 4

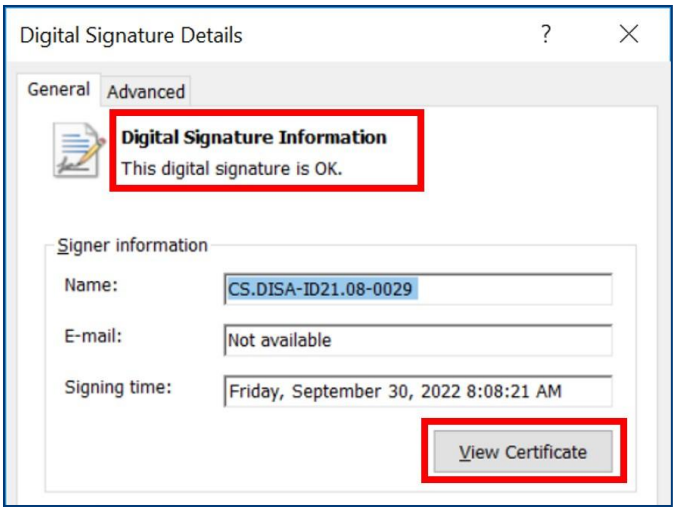
Select the name of the DoD PKE code signer (e.g. "CS.DISA-ID21.08-0029") in the **Signature list** and click **Details**. The **Digital Signature Details** window opens.



Continued on page 3

Step 5

Make sure that the "*This digital signature is OK*" message appears as shown. Click **View Certificate**.



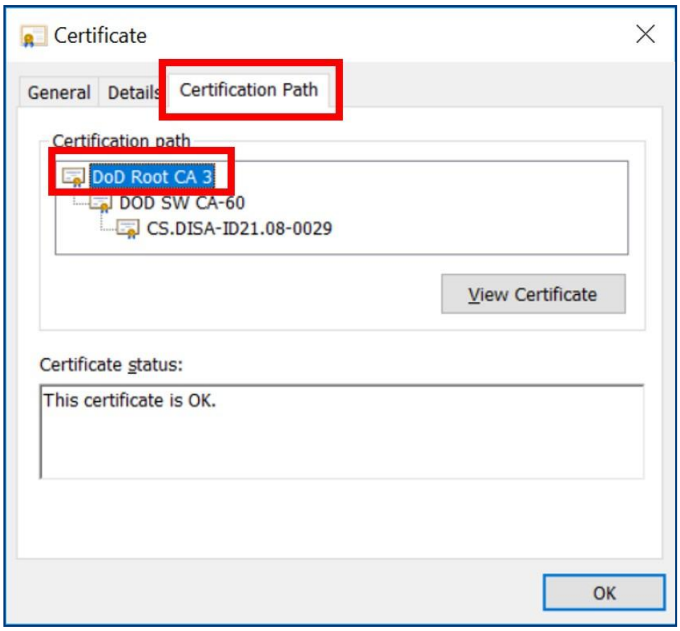
Step 6

Select the **Certification Path** tab to verify the certification path. The certification path should show DoD Root CA # (e.g. "DoD Root CA 3") at the top of the path, followed by a DoD subordinate CA (e.g. "DoD SW CA-60") and lastly list the DoD PKE code signing certificate name (e.g. "CS.DISA-ID21.08-0029").

If the digital signature is not OK, do not proceed with installation as the version of the tool you have may not be authentic.

NOTE: If the signature is listed as being invalid but the path appears to be correct (including a DoD Root CA), DoD PKI certificates may not be correctly configured on your system. Contact your local help desk or dodpke@mail.mil for assistance.

Click **OK** in each of the three open properties windows to close them.



For questions or comments regarding Public Key Enablement (PKE), please submit information to:

dodpke@mail.mil