# Dual Signing with a SHA1 Certificate and a SHA256 Certificate

## Dual Signing with a SHA1 Certificate and a SHA256 Certificate

## Introduction

In some cases, you might want to sign a driver package with two different signatures. For example, suppose you want your driver to run on Windows 7 and Windows 8. Windows 8 supports signatures created with the SHA256 hashing algorithm, but Windows 7 does not without an update (Microsoft, Availability of SHA-2 Code Signing Support for Windows 7 and Windows Server 2008 R2, 2015). For Windows 7, you need a signature created with the SHA1 hashing algorithm or to run the Windows Update

Suppose you want to build and sign a driver package that will run on Windows 7 and Windows 8 on x64 hardware platforms. You can sign your driver package with a primary signature that uses SHA256. Then you can append a secondary signature that uses SHA1. You can use the same certificate for both signatures, or you can use separate certificates.

Note that only PE files can be dual signed. (Microsoft, Appendix 4: Driver Signing Issues, n.d.) (Portable Executable, n.d.)

## Getting the Certificates

By default a DigiCert code signing certificate is SHA256. This guide assumes that you already have this certificate and have it installed to the signing machine. If you need help with this please refer to our code signing support page or contact us directly.

To get a SHA1 version of the code signing certificate is a pretty simple process, we can simply re-key the certificate in the online account.

1. Log into your DigiCert account, click on the 'My Orders' tab and then click on the corresponding order number.
2. Under "Reissue Options", choose the link to "Re-Key Your Certificate."
3. Select your server platform. To sign a driver in our example above we need to select Microsoft Kernel-Mode Code. Note that Sun Java is the only server platform that will require a CSR.
4. In the Advanced Options field uncheck Use a SHA-2 signature hash algorithm and click Continue to Next Step.
5. To finish the process, click the link to "Submit Request." When you submit your request to re-key the certificate an email is sent to the Certificate Requester to verify the request.
6. Before you can use your new certificate, you will need to follow the instructions in that email as per the initial code signing certificate installation.

## Verifying the SHA1 and SHA2 certificates

Once you have both certificates installed to the signing machine we need to determine which certificate is SHA256 and which certificate is SHA1. The process to verify what the certificate is can be fairly easy as well, but I do recommend running our DigiCert Certificate Utility for Windows to help with this process. Please follow these steps:

1. On your Windows workstation that you have the code signing certificate installed to the current user's Windows User Account, download and save the DigiCert Certificate Utility for Windows (DigiCertUtil.exe).
2. Run the DigiCert® Certificate Utility for Windows.
   Double-click DigiCertUtil.exe
3. In the DigiCert Certificate Utility for Windows, click Code Signing (blue and silver shield), select the certificate that you want to look at and then click View Certificate.
4. This will bring up a Certificate window where you can click the Details tab and look for the Signature hash algorithm to identify if the certificate is sha1 or sha256.
5. Once you have identified the certificate, you can right-click on the certificate and then click Edit friendly name. Good friendly names can help you easily identify each certificate at a glance.
6. In the Friendly Name box, enter a unique friendly name for the certificate to help you distinguish this certificate from the other certificates on your server. ie *yourCompany-(hash) (Company Name Inc-sha1 or Company Name Inc-sha256)*
7. Repeat the above steps to identify the second certificate.
8. When you are finished, click Save.

## Building the Signing Command

Now that we have identified the certificate we can start building the command that we need to use to sign the files with both certificates.

## Get Your Certificate’s Thumbprint

1. Run the DigiCert® Certificate Utility for Windows.
2. Double-click DigiCertUtil.
3. In DigiCert Certificate Utility for Windows©, click Code Signing (blue and silver shield), and right-click on your SHA256 code signing certificate, and then, click Copy thumbprint to clipboard. Then you may paste it in a text editor.
4. Repeat the above steps to get the thumbprint for the SHA1 certificate. (make a note on which thumbprint is which)

## How to Sign Authenticode Files with Your Authenticode Signing Certificates

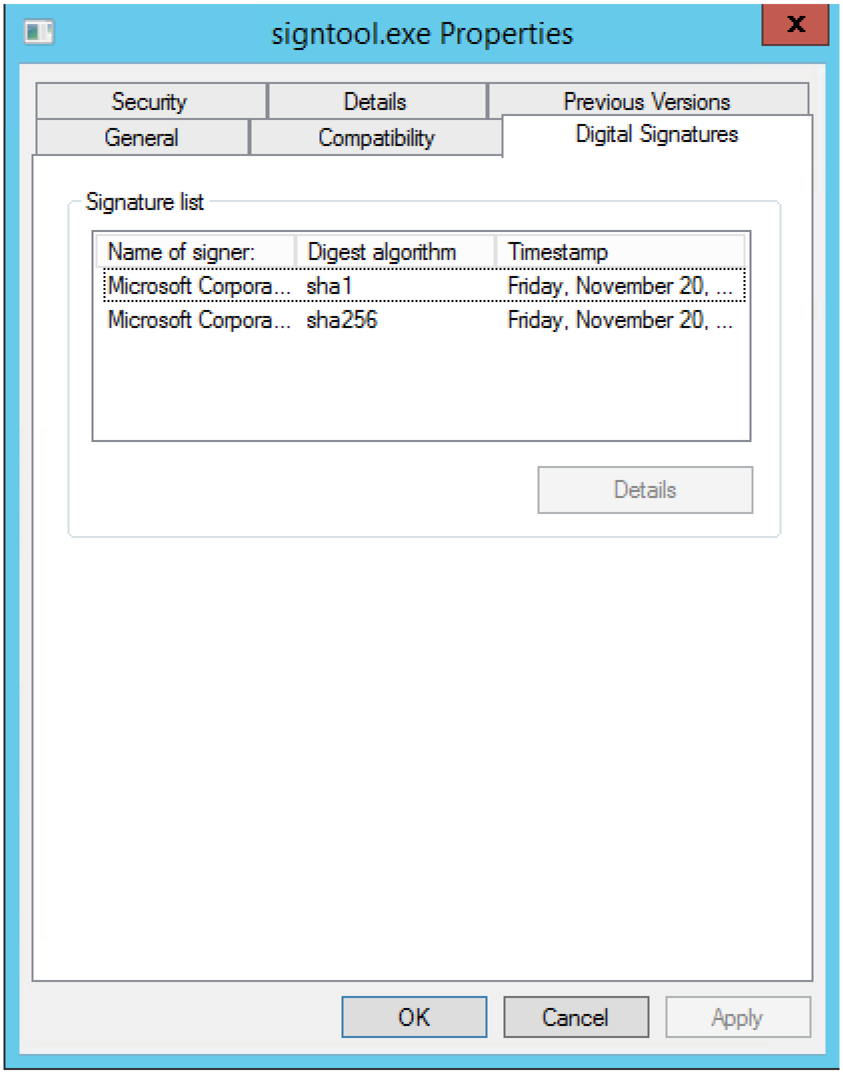
1. Open the Command Prompt as an admin.
    a. On the Windows Start screen, type cmd.
    b. Right-click on Command Prompt and then click Run as administrator.
    c. In the User Account Control window, click Yes to allow the program to make changes to the computer.
2. Run the following commands to apply the SHA1 signature and append the SHA2 signature:
    - `signtool sign /t http://timestamp.digicert.com /sha1 XXSHA1CERTTHUMBPRINTXX WINQUAL.EXE`

    - `signtool sign /tr http://timestamp.digicert.com /td sha256 /fd sha256 /as /sha1 XXSHA256CERTTHUMBPRINTXX WINQUAL.EXE`

      NOTE:
      XXSHA1CERTTHUMBPRINTXX is the thumbprint of your SHA1 code signing certificate
      XXSHA256CERTTHUMBPRINTXX is the thumbprint of your SHA2 code signing certificate
      WINQUAL.EXE is the executable file you want to sign
      For all of the command-line options for using SignTool, please see Microsoft's Signtool Documentation Page.

# How to verify the digital signature

You can verify that your application is now signed by right clicking on it and clicking Properties. On the Digital Signatures tab (if it exists), you can view the signing certificate and timestamp.



| Name of signer: | Digest algorithm | Timestamp |
|---|---|---|
| Microsoft Corpora... | sha1 | Friday, November 20, ... |
| Microsoft Corpora... | sha256 | Friday, November 20, ... |

## References

Microsoft. (2015, March 10). *Availability of SHA-2 Code Signing Support for Windows 7 and Windows Server 2008 R2*. Retrieved from https://technet.microsoft.com/en-us/library/security/3033929.aspx

Microsoft. (n.d.). *Appendix 4: Driver Signing Issues*. Retrieved from hardware Dev Center: https://msdn.microsoft.com/en-us/library/windows/hardware/dn741532%28v=vs.85%29.aspx

*Portable Executable*. (n.d.). Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Portable_Executable

Driver Signing Issues: https://msdn.microsoft.com/en-us/library/windows/hardware/dn741532%28v=vs.85%29.aspx

SHA2 Support Windows 2008 R2 and Windows 7: https://technet.microsoft.com/en-us/library/security/3033929.aspx

Signing a Driver for Public Release: https://msdn.microsoft.com/en-us/library/windows/hardware/hh967734%28v=vs.85%29.aspx

SHA1 Deprecation Policy: http://social.technet.microsoft.com/wiki/contents/articles/32288.windows-enforcement-of-authenticode-code-signing-and-timestamping.aspx